El Derecho de la Protección de Datos Personales y la Industria de la Salud Digital

Dña. Lorena Pérez Campillo

Tesis depositada en cumplimiento parcial de los requisitos para el grado de Doctor en

Derecho

Universidad Carlos III de Madrid

Directora: Dra. Dña. Teresa Rodriguez de las Heras Ballell

Diciembre 2019

DEDICATORIA

A mis padres. Por ser mi auténtico combustible y ser mis compañeros incondicionales, siempre, mis mentores de vida. A mis abuelas, por sus palabras, miradas y sonrisas llenas de amor. Y a mis abuelos, por darme su luz y protección.

A mis amigos y amigas por sus muestras de cariño y apoyo en los mejores y peores días. Son la gran familia que he podido escoger. Gracias por tanto.

A mi querida amiga y compañera de UC3M, Marie C. quien hace casi una década me transmitió las ganas de aprender e investigar en derecho comunitario cuando escapábamos al fondo de documentación europea para pasar tardes enteras sobre políticas europeas. Era una brillante jurista e investigadora y mejor persona. Le dedico con todo mi corazón mi tesis, allá donde esté.

AGRADECIMIENTOS

Son muchas las personas que han contribuido de forma directa o indirecta al proceso y conclusión de este trabajo.

En primer lugar, quiero agradecer a la profesora Teresa Rodriguez de las Heras Ballel, *directora de esta tesis* que me apoyara de manera personal y me alentara a desarrollar la idea inicial que tenía de la investigación. Desde el primer momento que la conocí supe que sería la mejor referencia que podría tener, no solo por sus líneas de investigación en cuestiones de derecho tecnológico alineadas a mi trabajo y por su brillante trayectoria académica y profesional sino también por sus cualidades personales únicas. En definitiva, ha sido un auténtico privilegio seguir sus recomendaciones y orientaciones a lo largo de estos -casi- cinco años.

En segundo lugar*, a mis mentores.* En particular, quisiera agradecer al profesor *Javier Puyol*, que me animara a presentar mi TFM al premio de las autoridades de protección de datos nacionales y que además, continuara la investigación a través de una tesis doctoral. También quisiera dar mi agradecimiento al profesor *Ricard Martínez,* quien de forma indirecta me ha enseñado tanto en investigación como en docencia en protección de datos durante el periodo del desarrollo de este trabajo. Por último, al investigador *Iñigo de Miguel,* quien me insistió en que participara en proyectos de investigación de protección de datos, tecnología y salud donde a día de hoy no paro de aprender. Posiblemente, me deje muchos por el tintero, pero me gustaría hacer este agradecimiento extensible a aquellos que puedan leer este trabajo en estos momentos y sepan que han colaborado de manera indirecta en este trabajo que empezó hace varios años.

CONTENIDOS PUBLICADOS Y PRESENTADOS

1. Libro colectivo: "*Fodertics 7.0 : estudios sobre derecho digital*".
Autora del Capítulo *"¿Blockchain como solución en la protección de datos personales y privacidad?"*
(Contribución parcial en la tesis doctoral. El material de esta fuente incluido en la tesis no está señalado por medios tipográficos ni referencias.)
ISBN:978-84-9045-765-8. Pp. 261-268. Editorial Comares. Coord. Por Irene González Pulido; Federico Bueno de Mata (Dir.) (2019). URL disponible aquí : (ult. fecha acceso: 14/4/2019).

2. Obra "*La convergencia de la tecnología y el Derecho*".
Autora del Capítulo *"La protección de datos en la E-Health: Especial mención al Big Data y al RGPD"*. Pp. 146 -155.
(Contribución parcial en la tesis doctoral. El material de esta fuente incluido en la tesis no está señalado por medios tipográficos ni referencias.)
ISBN:978-607-535-046-2. Editorial Universitaria. Dir. Carlos Eduardo Medina Guerrero (2018). Disponible URL aquí (ult. fecha acceso: 14/4/2019).

3. Obra colectiva: *Fodertics 6.0: los nuevos retos del derecho ante la era digital.*
Autora del Capítulo *"la nueva protección de datos en la e-Health: especial mención a los wearables"*
Pp. 95-106.
(Contribución parcial en la tesis doctoral. El material de esta fuente incluido en la tesis no está señalado por medios tipográficos ni referencias.)
ISBN: 978-84-9045-571-5. Editorial Comares. Coord. Por Federico Bueno de Mata. (2017). Disponible URL aquí (utl. fecha acceso: 14/4/2019).

4. Libro colectivo: *"Hacia una Justicia 2.0"*.
Autora del Capítulo *"Aspectos jurídicos del Cloud Computing: Gobernance & Risk & Compliance"* (2016). Pp: 229.241.
(Contribución parcial en la tesis doctoral. El material de esta fuente incluido en la tesis no está señalado por medios tipográficos ni referencias.)
ISBN: 978-84-16324-43-9. Editorial Ratio Legis. Director: Federico Bueno de la Mata. Volumen III, 2016. Disponible URL aquí (utl. fecha acceso: 14/4/2019).

5. Artículo *"El nuevo RGPD y cloud computing"*.
Revista digital IT USER (Enero 2017).
(Contribución parcial en la tesis doctoral. El material de esta fuente incluido en la tesis está señalado por referencias.)
Disponible aquí (ult. fecha acceso: 14/4/2019).

6. Artículo "Códigos de Conducta y Cloud Computing".
Revista digital IT USER (Diciembre 2016)
(Contribución parcial en la tesis doctoral. El material de esta fuente incluido en la tesis está señalado por referencias.)
Disponible URL aquí (ult. fecha acceso: 14/4/2019).

7. Artículo "La homologación de proveedores cloud" .
Revista digital IT USER (Noviembre 2016)
(Contribución parcial en la tesis doctoral. El material de esta fuente incluido en la tesis está señalado por referencias.) Disponible aquí (últ. fecha acceso: 14/4/2019).

CONTENIDOS PRESENTADOS NO PUBLICADOS.

1. Trabajo: *"Una aproximación al big data y al blockchain sanitario y su implicación en la protección de datos personales"*
   Institución: Universidad del País Vasco (UPV/EHU). Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada.
   Previsión de publicación: noviembre 2019.

2. Trabajo: *"Blockchain y RGPD. Un enfoque práctico para la Industria de la Salud"*.
   Solicitud de Premio de Investigación en Protección de Datos Personales Emilio Aced
   Institución: Agencia Española de protección de datos (AEPD)
   Año entrega del trabajo: 2019.

3. Trabajo: *"La nueva protección de datos y cloud computing: GRC, homologación y autorregulación de proveedores"*.
   Solicitud de Premio de Investigación en Protección de Datos Personales Institución: Agencia Vasca de protección de datos (AVPD)
   Institución: Agencia Vasca de protección de datos (AVPD)
   Año entrega del trabajo y obtención del premio: 2017.

4. Trabajo: *"La nueva protección de datos y cloud computing: GRC, homologación y autorregulación de proveedores"*.
   Solicitud de Premio de Investigación en Protección de Datos Personales Institución: Agencia Española de protección de datos (AEPD)
   Año entrega del trabajo: 2017.

   Nota: Los tres últimos son trabajos de investigación presentados en las Autoridades de control nacional y autonómica para ser candidata a los premios citados en las convocatorias citadas, siendo premiado el segundo trabajo por la AVPD (2017), el cual no ha sido publicado, salvo error.

INDICE

1.1.Introducción.

1.2.Riesgos y la protección de datos

1.3.Una aproximación a las posibles soluciones

2.INTERNET DE LAS COSAS DE LA SALUD.

2.1.Introducción

2.2.Clasificación del IoT de la salud

2.3.Riesgos y la protección de datos.

2.4.Una aproximación a las soluciones posibles.

3.BIG DATA DE LA SALUD

3.1.Introducción

3.2.Riesgos y la protección de datos.

3.3.Una aproximación a las posibles soluciones

3.4.Fases del proyecto big data aplicado al cuidado de la salud.

4.INTELIGENCIA ARTIFICIAL Y MACHINE LEARNING DE LA SALUD

4.1.Introducción.

4.2.Clasificación de IA en salud.

4.3.Riesgos y la protección de datos

4.4.Una aproximación a posibles soluciones

5.BLOCKCHAIN Y DLT EN SALUD.

5.1.Introducción

5.2.Clasificación de Blockchain

5.3.Aplicabilidad a la Atención Sanitaria: utilidades y casos reales.

5.4.Aplicabilidad a la Industria Farmacéutica: utilidades y casos reales.

5.5.Aplicabilidad en la Industria Aseguradora: utilidades y casos reales.

5.6.Fases del proyecto blockchain aplicado al cuidado de la salud.

5.7.Contexto futuro.

III. REGIMEN JURÍDICO DE LA PROTECCIÓN DE DATOS DE CLOUD COMPUTING E IoT DESDE EL ENFOQUE DE LA INDUSTRIA DEL CUIDADO DE LA SALUD DIGITAL.

1.RÉGIMEN JURÍDICO APLICABLE AL USO DE CLOUD COMPUTING DE LA SALUD

1.1.Los sujetos jurídicos

1.2.La contratación Cloud.

1.3.Transferencias internacionales y "BCR"

2. REGIMEN JURÍDICO APLICABLE AL USO DE IOT DE LA SALUD.

2.1.La importancia de la seguridad en la privacidad en IoT.

2.2.Los sujetos jurídicos implicados

IV. RÉGIMEN JURIDICO EN PROTECCIÓN DE DATOS DE BLOCKHAIN DESDE EL ENFOQUE DE LA INDUSTRIA DEL CUIDADO DE LA SALUD DIGITAL.

1.INTRODUCCIÓN

2.PARTICULARIEDADES JURÍDICAS GENERALES DE PROTECCIÓN DE DATOS EN BLOCKCHAIN Y DLT.

2.1.Los sistemas de gestión de identidad aplicables a blockchain

2.2.Los contratos inteligentes ("smart contracts")

2.3.Blockchain como herramienta de compliance.

3.PARTICULARIEDADES JURÍDICAS ESPECÍFICAS DE PROTECCIÓN DE DATOS EN BLOCKCHAIN Y DLT.

3.1.El tratamiento de datos personales y el consentimiento en blockchain.

3.2.El concepto de "dato personal" en blockchain.

3.3.Tipos de datos en Blockchain y DLT.

3.4.Los sujetos jurídicos en el tratamiento en blockchain.

3.5.Obligaciones de los sujetos jurídicos

3.6.Respecto a la privacy by design / by default

4.INCOMPATIBILIDADES CON RGPD Y APROXIMACIÓN A POSIBLES SOLUCIONES.

4.1.Respecto a la transparencia y la designación del responsable.

4.2.Respecto al principio de minimización de datos personales.

4.3.Respecto al derecho de rectificación.

4.4.Respecto al derecho de acceso

4.5.Respecto al derecho de supresión (o al olvido)

4.6.Aproximación a soluciones: Off chain y side chain

4.7.Aproximación a soluciones: Uso de IA de middleware.

4.8.Respecto a la limitación del plazo de conservación.

4.9. Respecto al equilibrio innovación tecnológica vs regulación.

V. COMPLIANCE Y RESPONSABILIDAD EN MATERIA DE PROTECCIÓN DE DATOS PARA APLICAR A LA INDUSTRIA DEL CUIDADO DE LA SALUD DIGITAL

1. LA GESTIÓN DE RIESGOS EN PROTECCIÓN DE DATOS.

1.1.La responsabilidad proactiva (“accountability”)

1.2.El análisis de riesgo.

1.3.La evaluación de impacto.

1.4.La gobernanza de datos

2. AUTORREGULACIÓN

2.1.Código- tipo de conducta

2.2.Autorregulación privada sectorial tecnológica.

2.3.Best practices corporativas.

3. CERTIFICACIÓN.

3.1.Sellos de privacidad

3.2.Certificaciones técnicas.

4. HOMOLOGACIÓN.

5. COMPLIANCE

5.1.Definición y características.

5.2.Responsabilidad, protección de datos y compliance.

5.3.Canales de denuncia ("whistleblowing")

6. RESPONSABILIDAD SOCIAL EMPRESARIAL O CORPORATIVA.

7. EL RÉGIMEN SANCIONADOR.

7.1.El régimen sancionador en el RGPD.

7.2.El régimen sancionador en la LOPDGDD.

7.3. EL DERECHO A INDEMNIZACIÓN Y RESPONSABILIDAD.

VI. EL DERECHO FUNDAMENTAL DE LA PROTECCIÓN DE DATOS PERSONALES . ENFOQUE DESDE EL ÁMBITO DE LA SALUD Y TECNOLOGÍA

1.INTRODUCCIÓN

2. EL DERECHO DE PROTECCIÓN DE DATOS COMO DERECHO DE LA PERSONALIDAD

3. BREVE ORIGEN DOCTRINAL Y JURISPRUDENCIAL DE LA PROTECCIÓN DE DATOS PERSONALES.

4. LA IMPORTANCIA DEL DERECHO DE PROTECCIÓN DE DATOS DE SALUD DIGITAL EN LA ERA TECNOLÓGICA.

VII. CUESTIONES PREVIAS Y EL NUEVO RÉGIMEN JURÍDICO EN MATERIA DE PROTECCIÓN DE DATOS EN SALUD Y TECNOLOGÍA

1. FLUJO DE DATOS DE SALUD EN EL MERCADO ÚNICO DIGITAL

2.OPEN DATA DE SALUD

3.REUTILIZACIÓN DE DATOS Y LA SALUD.

4.LOS METADATOS DE SALUD

5.LOS HISTORIALES MÉDICOS ELECTRÓNICOS

6.SALUD, TECNOLOGÍA Y EL DERECHO DE PROTECCIÓN DE DATOS

7.MENORES DE EDAD, SALUD, TECNOLOGÍA Y PROTECCIÓN DE DATOS

VIII. EL NUEVO RÉGIMEN JURÍDICO EN MATERIA DE PROTECCIÓN DE DATOS APLICADO A LA INDUSTRIA DEL CUIDADO DE LA SALUD DIGITAL

1.EL NUEVO MARCO NORMATIVO EUROPEO DE PROTECCIÓN DE DATOS

1.1.Antecedentes y proceso de reforma normativa europea

1.2.El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (RGPD)

2.EL NUEVO MARCO NORMATIVO ESPAÑOL DE PROTECCIÓN DE DATOS

2.1.Antecedentes de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD)

2.2.Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales(LOPDGDD)

3. LA NORMATIVA SECTORIAL ESPECÍFICA.

3.1.La Ley 14/1986, de 25 de abril, General de Sanidad.

3.2.El Reglamento eIDAS y la Directiva SRI

4. EL RÉGIMEN JURÍDICO TRATAMIENTO DE DATOS EN LA INVESTIGACIÓN BIOMÉDICA Y ENSAYOS CLÍNICOS

4.1. La investigación biomédica.

4.2. Investigación clínica no biomédica

4.3. Ensayos clínicos.

5. PARTICULARIDADES JURÍDICAS PARA PROYECTOS DE BIG DATA E INVESTIGACIÓN BIOMÉDICA

5.1.Origen de los datos

5.2.Finalidades

5.3.Derechos de los interesados.

5.4.Legitimación

5. 5.Decisiones individuales automatizadas

5. 6.Principios del RGPD aplicables. El papel de los desarrolladores.

5.7.Evaluaciones de impacto.

5.8.Medidas necesarias.

5.9.Buenas prácticas.

5.10.Retos y desafíos

5.11.Una aproximación a las posibles soluciones

PARTICULARIDADES JURIDICAS DE LAS ASEGURADORAS DE SALUD Y PROTECCIÓN DE DATOS A TENER EN CUENTA.

6.1.Finalidades del tratamiento de las aseguradoras.

6.2.Legitimación

6.3.Cesión de datos personales con finalidad de "selección de riesgos"

6.4. Recogida de datos personales de salud

6.5.Datos genéticos y aseguradoras.

IX. IMPLICACIONES ÉTICA*S* DESDE EL PUNTO DE VISTA DE LA PROTECCIÓN DE DATOS Y LA PRIVACIDAD EN LA INDUSTRIA DEL CUIDADO DE LA SALUD DIGITAL.

1. CONSIDERACIONES INICIALES.

1.1.Dataísmo, fuentes de datos de salud y stakeholders

1.2.La medicina participativa, el negocio farmacéutico y la ética (de datos).

1.3.Los derechos fundamentales, ética y privacidad.

2.IMPLICACIONES ÉTICAS Y DE LA PRIVACIDAD EN SALUD

2.1.Implicación ética con Big Data

2.2.Implicaciones éticas con IA.

2.3.Implicaciones éticas con IoT y m-Health.

2.4.Implicaciones éticas con Blockchain/DLT.

2.5.Implicaciones éticas del futuro: neuroinformática, neurotecnología y biohacking, informática cuántica y genética.

3.LA ETICA DE LOS DATOS Y LAS PERSONAS

3.1.Preocupación por la privacidad.

3.2.El titular como propietario del dato personal.

3.3.Mercado negro de datos de salud.

3.4.Datos personales para el bien común.

4.LA ÉTICA DE LOS DATOS Y LAS ORGANIZACIONES.

4.1.La ética de los datos y RSE

4.2.La ética impuesta

4.3.Comités de ética en empresas.

4.4.La necesaria autoevaluación.

4.5.Certificaciones y sellos de calidad de ética de datos.

4.6.Ética desde el diseño ("Ethic by design")

4.7.Los valores y la ética de datos.

4.8.La privacidad como valor.

4.9.Casos de estudio

4.10.Conclusión: "De las reglas a los valores, de la amenaza a la identidad corporativa".

5.LA ETICA DE LOS DATOS Y LAS INSTITUCIONES PÚBLICAS Y GOBERNANZA.

CONCLUSIONES

INFORMES Y DOCUMENTACIÓN OFICIAL

NORMATIVA

JURISPRUDENCIA

TABLAS E IMÁGENES

RECURSOS ELECTRÓNICOS

ABREVIATURAS

- AAPP Administraciones Públicas
- AIAs Guia de Evaluación de impacto algorítimicas
- ADN ácido desoxirribonucleico
- AEPD Agencia Española de Protección de Datos
- AI inteligence artificial
- APDCAT Autoridad de protección de datos catalana
- API *Application Programming Interface*
- app. aplicación móvil
- aprox. aproximadamente
- ARN ácido ribonucleico
- AVPD Agencia Vasca de Protección de Datos
- *AWS* *Amazon Web Services*
- BaaS *Blockchain-as-a-service*
- BCR *Binding Corporate Rules*
- BOE Boletín Oficial Español
- CAC Administración del Ciberespacio de China
- CC Código civil
- CCO *chief compliance officer*
- CE Constitución Española
- CEDH Convenio de Derechos Humanos
- CIF *Cloud Industry Forum*
- CNIL Comisión Nacional de la Informática y las Libertades (Francia)
- CSA *Cloud security alliance*
- CP Código penal
- CRISPR *Clustered Regularly Interspaced Short Palindromic Repeats*
- Dapp *Digitally Abled Producers Program*
- DAO *Decentralized Autonomous Organization*
- DDHH Derechos humanos
- DLT *Distributed Ledger Technology*
- DNI Documento nacional de identidad
- DPD Delegado de protección de datos
- DPO *Data protection officer*
- ECHI *European Core Health Indicators*
- EDPS *European Data Protection Supervisor*
- EEE Espacio Económico Europeo
- EHR *Electronic Medical Record*
- ej. ejemplo
- EIPD Evaluación de Impacto de Protección de Datos
- ENISA Empresa Nacional de Innovación Sociedad Anónima
- EPIS Equipo de protección individual
- Et. al y otros
- etc. etcétera
- EuroPriSe *European Privacy Seal*
- FCT Comisión Federal de Comercio norteamericano
- FDA *Food and Drug Administration* (USA)
- FDVT *Facebook Data Valuation Tool*
- FINH Fundación para los Institutos Nacionales de la Salud

- GRC *gobernance & risk & compliance*
- GT29 Grupo del Trabajo del Art.29
- HCE Historial clínico electrónico
- HIPAA *Health Insurance Portability and Accountability Act* (USA)
- HME Historial médico electrónico
- IA inteligencia artificial
- Iaas *Infraestructure as a Service*
- ibíd. citado en la cita previa
- ICB Comité Internacional de Bioética
- ICO *Information Commissioner's Office* (UK)
- ICO *Initial Coin Offerings* (oferta inicial de moneda)
- I+D Investigación + desarrollo
- IOTA *Intra-European Organisation of Tax Administrations*
- IoTM *Internet of Medical Things*
- IoTH *Internet of Health Things*
- ISO *International Standard Organization*
- ITU Unión Internacional de Telecomunicaciones
- LIB Ley de Investigación Biomédica
- LPAC Ley Procedimiento Administrativo Común de las Administraciones Públicas
- LOPD Ley Orgánica de Protección de Datos
- LOPDGDD Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales
- LOPJM Ley Orgánica de Protección de Menores
- LORTAD Ley Orgánica
- NHS *National Health Service* (UK)
- NIST *National Institute of Standards and Technology*
- OCDE Organización para la Cooperación el Desarrollo Económico)
- OMS Organización Mundial de la Salud
- ONGs Organización No Gubernamental
- ONTSI Observatorio Nacional de las Telec. y Sociedad Información
- ONU Organización de Naciones Unidas
- Paas *Platform as a Service*
- PDA asistentes digitales personales
- PLA *Privacy Level Agreement*
- PIMB países de ingresos bajos y medios
- PIB Producto interior bruto
- pp páginas
- PRL Prevención de riesgos laborales
- PYME Pequeñas y medianas empresas
- p.e. por ejemplo
- RGPD Reglamento General de Protección de Datos
- RRSS Redes sociales
- RSE Responsabilidad social empresarial
- RSC Responsabilidad social corporativa
- Supra cit. citado anteriormente, mencionado arriba.
- Saas *Software as a Service*
- SC *Smart Contracts*
- SECOT Sociedad Española de Cirugía y Traumatología
- SEOM Sociedad Española de Oncología Médica

- SEPD Supervisor Europeo de Protección de Datos
- SLA *Service Level Agreement*
- SSI Sistema de Identificación Soberana
- STC Sentencia del Tribunal Constitucional
- STS Sentencia del Tribunal Supremo
- TEDH Tribunal Europeo de Derechos Humanos
- TIC Tecnologías de la Información y Comunicación
- TJUE Tribunal de Justicia de la Unión Europea
- UE Unión Europea
- USA *United States of America*
- UDBHR Declaración Universal sobre Bioética y Derechos humanos
- UNESCO *United Nations Educational, Scientific and Cultural Organization*
- Vid. veáse
- VIH virus de la inmunodeficiencia humana

RESUMEN

Tecnologías como cloud, big data, IA, IoT o computación cuántica *impactan de lleno con el derecho fundamental* de protección de datos. La cuestión se agrava cuando se habla de información de salud de personas que puede condicionar la vida de las mismas en situaciones cotidianas como una solicitud de un seguro interactivo de salud, un empleo o una hipoteca.

Esa información tiene una *clara dimensión económica*, más allá y al margen de la búsqueda del bien común de una sociedad desarrollada y con calidad de vida, tanto para proveedores farmacéuticos o tecnológicos como para las personas. Existen ejemplos de ello. Respecto al primer caso, nos referimos a una empresa de genética y al "mercadeo" de datos de miles de pacientes (de un valor total de 48 millones de euros) o a empresas farmacéuticas que podrían comprar paquetes de datos de pacientes (de un valor de 441 euros aprox./persona). Y es que cada vez es más frecuente encontrarse con consorcios formados por gigantes tecnológicos e industrias farmacéuticas para obtener mayor rentabilidad en sus negocios. En cualquier caso, partiremos de la premisa de que los intereses económicos no deberán primar sobre los derechos y libertades de las personas. Y en el segundo caso, nos referimos a que las personas, dentro de poco también van a poder "monetizar" sus datos personales a *través de blockchain*, bien como recompensa económica o bien en forma de descuentos de servicios o productos.

En otro orden de cosas, no podemos ignorar las *dificultades* que existen para *regular la tecnología,* debido a la escasa especialización y capacitación del legislador, como se ha podido ver con el RGPD y su aplicabilidad en blockchain (con el derecho de supresión, portabilidad, etc.). Además, a medida que vayan llegando *avances tecnológicos*, más complicado será desarrollar un marco jurídico, piénsese p.e. en la deep learning de smartphones que leen la mente con IA , a la neurotecnología que ponen en peligro la "privacidad mental" o a la computación cuántica que hará desaparecer la ciberseguridad conocida hasta la fecha. Pero esa falta de especialización también toca al mercado laboral en donde escasean profesionales expertos en ética de los datos y privacidad o en tecnologías blockchain, posiciones del futuro según el Informe EPYCE.

A pesar de esto último, el escenario no es tan pesimista. Por ejemplo, surge la tendencia hacia un "modelo de autogestión de la información personal de salud" del individuo y las organizaciones cuentan con *medios autorregulatorios* en materia de seguridad y privacidad de la información, de ética empresarial y RSC donde los valores tienen un gran peso. En estas organizaciones e instituciones trabajan comités de ética con equipos multidisciplinares (ingenieros, economistas, matemáticos, filósofos, juristas, físicos, etc..).

El *soft law* y la autorregulación corporativa serán instrumentos útiles y necesarios para paliar el atraso de la máquina legisladora frente a la tecnología. Ahora bien, la ética y la legalidad deberán encajar y complementarse de la mejor manera posible. En cualquier caso, se requerirá de un diálogo entre *stakeholders* que ayude a eliminar el mito de que el derecho pone freno a la innovación, sin la cual no podría ser posible una sociedad desarrollada y con mejor calidad de vida.

Ante escenarios dinámicos; soluciones flexibles y creativas basadas en ética y cumplimiento normativo.

Palabras clave:

Protección de datos personales; RGPD; Industria del Cuidado de la Salud; Industria Farmacéutica, Sector Asegurador de Salud, Big Data; IA; IoT; Blockchain/DLT; Compliance; Ética de los datos.

ABSTRACT

Technologies such as cloud, big data, IA, IoT or quantum computing have a full impact on the fundamental right to data protection. The issue is aggravated when we talk about health information of people that can condition their lives in everyday situations such as an application for an interactive health insurance, a job or a mortgage.

This information has a clear economic dimension - beyond the search for the common good of a developed society with a quality of life- for pharmaceutical or technological providers as well as for individuals. For example, in the first case, we refer to a genetics company and the "marketing of data" from thousands of patients (EUR 48 million) or to pharmaceutical companies that could buy packages of patient data (for 441 € approx./person). It is becoming more and more frequent to find consortiums formed by technological giants and pharmaceutical industries in order to obtain greater profitability in their businesses. In any case, we will start from the premise that economic interests should not take precedence over people's rights and freedoms. And in the second case, persons will soon also be able to "monetize" their personal data through blockchain, either as a financial reward or in the form of discounts on services or products.

On the other hand, we cannot ignore the difficulties that exist to regulate technology, due to the scarce specialization and training of the legislator, as has been seen with the GDPR and its applicability in blockchain (with the right of to be forgotten, portability, etc.). In addition, as technological advances arrive, it will be more complicated to develop a legal framework, think e.g. deep learning of smartphones that read the mind by AI, neurotechnology that endanger "mental privacy" or quantum computing that will make disappear the cybersecurity known to date. But this lack of specialisation also affects the labour market, where there is a shortage of professionals with expertise in data ethics and privacy or in blockchain technologies, positions of the future, according to the EPYCE report.

Despite the latter, the scenario is not so pessimistic. For example, there is a trend towards a "model of self-management of personal health information" of the individual and organizations have self-regulatory means in terms of information security and privacy, business ethics and RSC where values carry great weight. In these

organizations and institutions, ethics committees work with multidisciplinary teams (engineers, economists, mathematicians, philosophers, jurists, physicists, etc.).

Soft law and corporate self-regulation will be useful and necessary instruments to alleviate the backwardness of the legislative machine in the face of technology. Now, ethics and legality must fit together and complement each other in the best possible way. In any case, a stakeholder dialogue will be required to help dispel the myth that law holds back innovation. Without technology there could not be a developed society with a better quality of life.

Therefore, the best option in dynamic scenarios is to use flexible and creative solutions based on ethics and regulatory compliance.

Keywords:

Privacy; GDPR; Healthcare Industry; Pharmaceutical Industry; Health Insurance Sector; Big Data; AI; IoT; Blockchain/DLT; Compliance; Accountability; Data Ethics.

INTRODUCCIÓN

1. PLANTEAMIENTO DEL PROBLEMA.

La Industria del Cuidado de Salud está experimentando una fuerte transformación digital con la llegada de tecnologías emergentes como Cloud Computing, Big Data. Inteligencia Artificial, Internet de las Cosas, Blockchain o incluso, Computación Cuántica. Este desarrollo tecnológico propicia inevitablemente mayor flujo o tráfico de información de salud, incluyéndose la información de personas físicas. De este avance tecnológico en la Sociedad de la Información que vivimos ya tomó consciencia el legislador comunitario europeo con la aprobación del Reglamento General Europeo de Protección de Datos.

Ahora bien, no se pueden ignorar las *dificultades* que existieron a la hora de "*regular la tecnología",* motivada posiblemente por la escasa especialización y capacitación de los legisladores en la materia[1]. Esta situación podría agravarse con la llegada nuevos avances tecnológicos, lo que hará más complicado desarrollar un marco jurídico deseable. Piénsese, por ejemplo, en la *deep learning* de smartphones que leen la mente gracias a inteligencia artificial a la neurotecnología que ponen en peligro la "privacidad mental" o a la computación cuántica que hará desaparecer la ciberseguridad conocida hasta la fecha; ¿cómo podrían los legisladores otorgar seguridad jurídica si la tecnología no tiene límites y avanza más rápido que la máquina legisladora?

Los marcos regulatorios actuales no parecen, a priori, otorgar soluciones legales totalmente eficaces donde se pueden regular los derechos fundamentales de las personas en el impacto de las personas en el ámbito de la Sociedad de la Información.

Por todo ello y por más factores, es el momento más oportuno (y necesario) para que la comunidad académica e investigadora estudie diferentes formas de protección legal para los titulares de datos dentro del contexto de la Industria de la Salud digital. Se requieren de mecanismos y sistemas protectores que aboguen por la defensa de los más vulnerables, es decir, de las personas físicas, frente a los intereses económicos empresariales.

[1] Esto se ha venido reflejado, por poner un ejemplo, a la hora de poder aplicar ciertos derechos de los titulares como los de rectificación, supresión o portabilidad (veáse art. 16, 17, 20 RGPD) en tecnologías como blockchain.

No resulta una tarea nada baladí por diferentes motivos que se procuran asumir desde el momento inicial de este trabajo. En primer lugar, cabe prevenir al lector de la gran importancia del derecho de protección de datos como derecho fundamental para las personas. Los datos personales de la salud son inevitablemente más sensibles que el resto de datos personales. En segundo lugar, por ejemplo, se requerirá de cierta delicadeza a la hora de analizar el impacto de las tecnologías en este derecho en relación con los beneficios que acarrean –inevitablemente- el desarrollo e innovación en una sociedad que persigue la mayor calidad de vida de las personas. En tercer lugar, por ejemplo, también, se necesitará de cierta observancia o creatividad para desarrollar sistemas de protección legal proactivos y casi "nuevos" hasta la fecha, que no obstante, han sido introducidos en las nuevas normativas (por ejemplo, instrumentos de compliance y ética empresarial).

Dicho lo anterior, y concluyendo este apartado, permítanme que haga especial énfasis a los siguientes cuatro extremos: a.) la *desprotección del titular de datos de datos de salud* en el contexto tecnológico del que hablamos, por ejemplo, manifestándose en forma de sesgos discriminatorios (ej. piénsese en el rechazo de pacientes de aseguradoras tras haber notificado su dispositivo wearable que no supera un mínimo de pasos diarios, o el estudio por parte de una aseguradora digital que potenciales asegurados en sus redes sociales han expresado su malestar físico generado por su enfermedad crónica etc..) ; b) las grandes cantidades de dinero que generan los *datos* (nuevo petróleo del S.XXI), también de salud. Hay noticias y estudios que señalan que un paquete de datos de salud de un paciente puede valorarse en 441 euros aprox. y un registro de salud, 13 euros aprox. por paciente ; c) y por último, el poder indiscutible de la *Industria de Salud* respecto a otras industrias o sectores; d) la reciente alianza de esta Industria con la tecnología (por ejemplo, piénsese en la posibilidad de extraer *"inteligence"* a través de analítica avanzada traduciéndose en monetización de la información). Y es que "los avances en IA hacen que sea más fácil para las compañías obtener acceso a los datos de salud, lo que aumenta la tentación de que las empresas los utilicen de manera ilegal o no ética". La consultora *Gartner* ya predijo en su momento que en el 50% de los negocios se producirían "*violaciones de ética"* debido al uso indebido de *big data*.

Habiendo abordado la problemático, procedamos a exponer la motivación de esta investigación.

2. MOTIVACIÓN DE LA INVESTIGACIÓN.

Es un buen momento para sacar esta línea de investigación a la luz de la comunidad académica, del sector privado e incluso del sector público. El escenario normativo es reciente y no existe, por el momento, a mi humilde modo de ver, suficiente literatura académica en relación con el impacto de tecnologías (como blockchain/DLT o biohacking o *smart pills*) en el marco de la Industria del Cuidado de la Salud Digital. También, resultaba conveniente presentar y "familiarizar" a los diferentes stakeholders implicados, términos antes nunca escuchados como son "legal design" (diseño legal), "data ethics" (ética de los datos), "compliance" (cumplimiento normativo), "accountability" (responsabilidad), etc.. entre otros que abordaremos. Es anecdótico pensar que los ejemplos que se sacan a la luz para introducir el alcance disruptivo de la tecnología en la mayoría de eventos del sector tecnológico o de la Industria tienen que ver con salud (p.e. lentillas y relojes inteligentes, cirujanos robots, etc.). Sin ánimo de extenderme en exceso, creo conveniente dar alguna pincelada a los antecedentes personales que propiciaron el nacimiento de este apasionante trabajo para procurar una posible conexión con motivaciones generales concretas.

Al finalizar el postgrado[2], fue cuando inicié la andadura en el camino de la investigación acerca del impacto de la tecnología cloud computing en el derecho de la protección de datos. Esta fue la temática que abordé en el trabajo de fin de Máster, en el que pude obtener una calificación de matrícula de honor. Tras haber dejado abiertas líneas futuras de investigación, opté por continuarla, ampliando hipótesis y posibles respuestas, presentando el resultado a la Agencia Vasca de Protección de Datos (AVPD) teniendo, además, el privilegio de recibir el accésit de premio de investigación al trabajo *"La nueva protección de datos y cloud computing: GRC, homologación y autorregulación de proveedores"* en 2017.

[2] En concreto, puedo decir, que el interés sobre la "*digitalización* del sector del cuidado de la salud" despertó claramente en el Congreso del año 2015 de la Asociación Expertos Nacionales Abogados de las Nuevas Tecnologías, cuando aún no había finalizado mis estudios del Máster de Abogacía Digital de la Universidad de Salamanca, al ver una diapositiva en la que se exponía una simple lentilla inteligente de Google.

Ahora bien, la motivación de enfocarlo en la *transformación digital de esta Industria de la Salud*[3], se inició una vez procesada la problemática general llegando a la conclusión de que el mayor impacto en los derechos y libertades de las personas se produciría en el momento en el que éstas no otorgaran la suficiente importancia al valor de sus datos, a su privacidad o intimidad, en el ámbito de la salud, mayoritariamente. Esto ocurriría cuando en el "ejercicio de ponderación" personal tuviera más peso la propia "recompensa" dirigida a, por ejemplo, ayudar al avance de una investigación médica de una enfermedad crónica o para obtener descuentos en las prima de un seguro de salud que el valor de su privacidad y de sus datos.

Fue en ese momento cuando descubrí la existencia de apps en las que intervenían gigantes de la industria farmacéutica –aliándose con tecnológicas- generando altos ingresos o la existencia de empresas (con página web) que monetizaban datos genéticos. Me gustaría dar al lector un dato importante. En el 2015, los *datos genéticos* de *23andMe* valían 2.500 veces más por usuario que los de Facebook. La empresa, por ejemplo, *Genentech* pagaría hasta 48 millones de euros por acceder a los 3.000 pacientes de Parkinson con base de datos de *23andMe.* También me conmovió conocer el caso Boehringher -del que muy poca información hay- y del que de alguna manera he querido hacer eco de forma abreviada en este trabajo.

En cualquier caso, no hay que perder de vista que el problema no está tanto en la discusión de si se podría poner freno al tráfico o flujo de información personal a determinados actores (para fines de investigación, etc. o no), sino en estudiar la trazabilidad de estos flujos de información, analizar los agentes que participan, sus responsabilidades y proteger a los titulares de los datos en el marco de la Sociedad de la Información en la que vivimos. Las tecnologías que han ido siendo objeto de estudio no dejan de ser "canales" donde la información personal se almacena, y, por tanto, cuanto más crezca, mayor será el impacto en las personas, y en la sociedad en su conjunto.

En la última etapa de investigación (a finales del año 2018 al 2019) fue cuando pude descubrir sorprendentes avances tecnológicos. Me refiero al "*Ping an Good*

[3] La motivación personal de enfocar y contextualizar el *derecho de protección de datos en el sector de Salud* vino exactamente en el momento que impartí docencia en el Máster Universitario de Protección de Datos (UNIR) la asignatura de Salud e Investigación Biomédica en el 2017. Es en ese momento cuando me di cuenta la cantidad de *stakeholders* que se ven afectados en el escenario de estudio. A los alumnos les costaba identificar casos o escenarios reales (por ejemplo, en la unidad de "Big Data"). Por lo que me hizo pensar que aún quedaba mucho por trabajar en este sentido.

Doctor"[4] de China o a las cápsulas de salud de inteligencia artificial de Dubai[5] o los avances en el ámbito de la Neurotecnología[6]. Y es que como señala un estudio de Gartner en el año 2020, el *ser humano va a ser un nodo activo de la red IP* donde se espera que a medio plazo, 14 trillones de dispositivos estarán conectados a alguna red.

Al entrar a formar parte como investigadora contratada de la Universidad del País Vasco (UPV/EHU) en el 2019 en la Cátedra de Genoma Humano y Derecho, pude descubrir de primera mano el entramado de actores a los cuales me refiero. Me percaté de las diferentes posibilidades de consorcios entre tecnológicas, farmacéuticas y/o laboratorios, investigadores, hospitales, universidades, asociaciones de pacientes o usuarios, gobiernos etc., donde la responsabilidad de los datos era esencial. En este marco se apostó por la difusión del conocimiento en relación con los *data cloud y blockchain* y la protección de datos en salud, donde pude colaborar humildemente en el marco del proyecto PANELFIT. Por ejemplo, en este sentido, este trabajo podría servir de apoyo en alguna medida para que colegas investigadores puedan desarrollar artículos de investigación de *smart pills* (o pastillas inteligentes) o de computación cuántica en la industria farmacéutica abordando riesgos legales en materia de protección de datos. Las necesidades de continuar esta línea de investigación por parte de la comunidad académica son evidentes y claras. El camino, no obstante, es largo pero las instituciones comunitarias están concienciadas de la necesidad de investigar en protección de datos para transmitir cierta "cultura de protección de datos y privacidad" a la ciudadanía consumidora de esta Industria o incluso a los propios investigadores de la comunidad científica que desarrollan su actividad en marcos totalmente tecnológicos como la inteligencia artificial.

---

[4] Proyecto consistente en "cabinas - consultorios portátiles a pie de calle" en China, donde los pacientes acuden para recibir atención primaria, en el cual se utilizan datos procedentes de 300 millones de consultas previas y recopila interactuando a través de texto y voz todos los síntomas y el historial médico del paciente. Posteriormente se realiza una sugerencia de diagnóstico preliminar donde un médico real mediante videoconferencia supervisa o corrige las conclusiones de IA y aporta comentarios complementarios.

[5] Las cuales cuentan con escáner digital de autoservicio que permite 19 mediciones rastrando indicadores de salud vitales en sólo 10 minutos en Dubái y están instaladas en centros comerciales o supermercados. Lo más novedoso es que medio de smart contract existe un sistema de recompensa (podría ser económica) donde los pacientes con buen comportamiento de salud reciben un token ("*body health utility token").*

[6] En los cuales se puede introducir información al propio cerebro o modelos experimentales de *"brain password"* que funcionan como *sistema biométrico cerebral* equiparable al sistema de autenticación móvil, o experimentos donde se ha introducido información gráfica en ADN como si se tratara de un pen-drive.

Por otro lado, también tuve el privilegio de participar como miembro del grupo de expertos en una fundación académica para el estudio de innovación y tecnología para pacientes. Gracias a este proyecto pude recoger una perspectiva global y transversal sobre los derechos de los pacientes/usuarios. Se tratan de grupos de trabajo multidisciplinares formados por personal sanitario y académico de gran prestigio y reconocimiento, de economistas de la salud, de funcionarios, de trabajadores de la Industria Farma, etc., lo que hace que las aportaciones en el ámbito jurídico y de la protección de datos y salud digital puedan resultar de necesidad y de interés, sobre todo cuando se habla de innovación o tecnología.

Y por último, también fui invitada a participar en la comisión de investigación de ética cuántica (en la *Quantum World Association*). En ésta estudiamos los riesgos ético-jurídicos de la tecnología cuántica, entre otras cuestiones, en lo relacionado con su impacto en la Industria de la Salud, concretamente para la Industria Farma.

Llegados a este punto, resulta conveniente dar mi más sincero agradecimiento a cada una de estas instituciones -y a las personas que les representan- por las que fui invitada a participar. Ha sido absolutamente enriquecedor. En ellas he podido percibir el interés y la necesidad que despierta esta línea de investigación en la Academia, en las Instituciones Comunitarias, en el Sector Privado de la Industria, e incluso, en gobiernos y Administraciones Públicas quienes, a mi humilde modo de ver, continuarán invirtiendo e interesándose en el futuro a corto y largo plazo. También en la firma de mi consultoría pude conocer interesantes y complejos proyectos tecnológicos (big data, Internet de las cosas, blockchain) que requerían consultoría (nada simple) en materia de protección de datos. Aún la normativa es reciente y la tecnología cada vez es más compleja por lo que la ultra especialización en las consultorías o firmas de despachos jurídicas se torna imprescindible.

En definitiva, a medida que el trabajo llegaba a su fin, más firmes eran mis argumentos respecto a la temática, no obstante, también era consciente de la delicadeza que entrañaría profundizar en una industria tan potente como la estudiada, donde mi última pretensión sería cuestionar la labor de esta Industria (aliándose con la tecnología), sino todo lo contrario. Y es que sin intención de anticiparme al desarrollo de las conclusiones quisiera transmitir al lector, mi optimismo respecto al posible

escenario de convivencia entre el Derecho, Tecnología e Innovación y el desarrollo de una sociedad sana y saludable.

3. OBJETO DE ESTUDIO Y OBJETIVOS.

El *objeto de estudio* es el derecho fundamental de protección de datos de salud en el ámbito de la Industria del Cuidado de la Salud digital, abordando el contexto del la Industria Aseguradora, la Industria Farmacéutica o el propio sector de la Atención Sanitaria. Se hará especial mención al compliance o cumplimiento normativo y a la ética (de los datos) como posibles herramientas para proteger a los titulares de datos. No podemos desdeñar que el objeto de estudio es totalmente multidisciplinar:

- Derecho: Principalmente nos referimos a Derecho Público (Derecho Constitucional pero también a Derecho Administrativo) pero también está presente el Derecho Privado (Derecho de los Negocios, Derecho Penal y Derecho Sanitario).

Aunque en menor medida, también estarán presentes las disciplinas de :

- Economía (de la salud y de la tecnología): Abordando la Industria del cuidado de la salud en el ámbito económico. Ver capítulo I y II.

- Tecnología: En especial se estudiarán cuestiones introductorias de las tecnologías cloud, IA, IoT, blockchain/DLT, entre otras. Ver capítulo II.

- Sociología: Analizando cuestiones referidas a las personas, organizaciones empresariales, o a las políticas públicas. Ver capítulo IX.

- Medicina: En concreto se hará especial hincapié en las cuestiones referentes a la protección y seguridad de la información personal de los pacientes o personas físicas. Ver capítulo I y VII.

Ahora bien, los *objetivos generales* más importantes de este trabajo son:

a. Observar, estudiar, analizar y desarrollar la problemática de estudio centrada en la *vulneración del derecho fundamental de la protección de datos* en el ámbito de la

Industria del cuidado de la Salud digital centrándose principalmente en el sector privado.

b. Analizar y distinguir las particularidades entre el Sector de Atención Sanitaria, la Industria Aseguradora de la Salud y la Industria Farmacéutica en el contexto digital.

c. Estudiar y analizar las *diferentes tecnologías presentes* en la Industria del cuidado de la Salud digital e incluso, las diferentes combinaciones entre ellas. Además, se abordará el impacto jurídico- económico de las mismas.

d. Analizar el *nuevo marco regulatorio de protección de datos* en el escenario de la Industria del cuidado de la Salud digital

e. Estudiar otras posibles soluciones jurídicas *("y no jurídicas")* al margen de las existentes que protejan a los titulares de datos personales de salud de esta Industria.

Los *subobjetivos* más importantes de este trabajo son:

a. Estudiar el impacto del big data, también, en la investigación científica.

b. Analizar el impacto de deep learning de la salud en el derecho fundamental de protección de datos de las personas.

c. Analizar el impacto de las tecnologías en el futuro, haciendo especial mención a Blockchain/ DLT como solución a la vulneración de del derecho. Iniciar análisis de paradigma de la Industria de Salud del futuro; Iota, Internet del ADN, computación cuántica, post humanismo, biohacking, biotecnología, etc.

d. Estudiar aspectos de compliance y responsabilidad afectos con el impacto de las tecnologías en salud en los derechos de las personas, en concreto, la gestión de riesgos, la autorregulación, la certificación, la homologación, el compliance, la responsabilidad social corporativa, el régimen sancionador y el derecho a indemnización.

e. Estudiar cuestiones relacionadas con el flujo de datos de salud en el mercado único digital, el open data de salud, la reutilización de datos de la salud, los metadados, los historiales médicos electrónicos, etc.

f. Analizar el régimen jurídico en materia de protección de datos personales. Analizar el cuerpo normativo del RGPD y LOPDGDD afecto a los datos de salud, y específicamente, en el contexto digital.

g. Desarrollar lo relativo a la necesidad imperiosa de la ética de los datos y su impacto en las tecnologías estudiadas dentro del contexto de la Industria del Cuidado de la Salud digital, todo ello en relación a las personas, a las organizaciones, y a las instituciones públicas y de gobernanza.

4. MARCO TEÓRICO Y METODOLÓGICO

4.1. Marco teórico y preguntas de investigación.

Sin intención de acotar una serie limitada de preguntas de investigación, se podrían citar las siguientes:

Respecto a la Industria del cuidado de la salud y tranformación digital y consideraciones específicas de las tecnologías.

1. Sería conveniente estudiar las *repercusiones y las perspectivas de futuro* que presentará la Industria, haciendo especial énfasis en la transformación digital de la industria farmacéutica y de la industria aseguradora (interactivas) en relación con los flujos de información y los datos como activo en sus compañías.

2. También resultaría de interés analizar la existencia o no sobre consorcios o convenios de aseguradoras con tecnológicas y proveedores de salud que realizan con el fin de *rentabilizar el negocio.* Ahora bien, las repercusiones para las personas titulares de datos pueden ser considerables; ¿serían legítimos los tratamiento de datos y hasta qué punto?

3. Analizar la política de privacidad de una aseguradora interactiva real. Ejemplo: Vivaz

4. Sería necesario analizar acerca de la legitimación de las decisiones automatizadas de datos personales por parte de las aseguradoras interactivas, en qué ocasiones estarán permitidas y los requisitos para ello.

5. ¿Qué soluciones, a priori, se podrían vislumbrar, respecto a la Industria, la tecnología y el derecho de protección de datos personales?

Respecto al régimen jurídico en protección de datos de cloud computing e IoT desde el enfoque de la Industris del cuidado de la salud digital.

6. Resultará de interés aportar un análisis respecto al impacto de cloud computing en los titulares de los datos.

7. Otra cuestión que requiere de su observación tiene que ver con los contratos de adhesión de cloud computing en esta Industria y en otras. Los proveedores cloud (ej. Microsoft) tienen clientes como centros sanitarios con los que formalizan contratos de servicios determinados, por lo general, con contratos tipo y de adhesión, donde en pocas ocasiones cabe negociación alguna salvo que se traten de clientes grandes (descartando las pymes sanitarias, por ejemplo); ¿qué consecuencias puede tener todo ello?

8. Además, habría que analizar las implicaciones que tienen las subcontratación en cloud para las personas o titulares de datos.

9. Por otro lado, pasemos a Internet de las cosas de la salud. Para analizar las responsabilidades que corresponden a cada uno de los sujetos jurídicos convendrá identificar los diferentes agentes que participan en la cadena de suministro donde se producen los flujos de información personal; fabricantes de dispositivos (ej. Fitbit), desarrolladores de API, subproveedores como redes sociales, etc.…

10. Resultaría de interés para el objeto de esta investigación, encontrar situaciones reales de aplicaciones y de seguros interactivos que pusieran de alguna manera en riesgo el derecho de protección de datos de las personas por el uso de éstos.

Respecto al régimen jurídico en protección de datos de blockchain desde el enfoque de la Industria del cuidado de la salud digital.

En otro orden de cosas, la tecnología "de moda", Blockchain *(en salud)* donde a priori, me surgen algunos interrogantes[7]:

[7] Pero también surgen otras cuestiones de investigación. Como por ejemplo, ¿podrá blockchain servir como herramienta poderosa *en materia* de *compliance y protección de datos* permitiendo demostrar el cumplimiento legal en la recogida del consentimiento por parte del responsable, la realización del documento de EIPD o análisis de riesgos o el propio uso de encriptación (innato a su naturaleza técnica)? Y lo que más interesante me parece, ¿podrán proporcionar evidencias de legitimación en entornos de

11. Identificar quiénes son los responsables y quiénes son los encargados del tratamiento de datos personales, subencargados y titulares de datos.

12. Analizar la forma de asignar responsabilidades a los sujetos jurídicos implicados.

13. Estudiar cómo podría beneficiar blockchain como gestor de control de acceso y permisos para datos y registros de salud a los titulares de datos personales.

14. Visto lo anterior, quedaría la parte más importante en relación con la compatibilidad del RGPD y esta tecnología; (d.1.) ¿Será compatible el derecho de rectificación? (d.2.) ¿Se podría hablar de posibles exenciones a las obligaciones por motivos de limitaciones técnicas? (d.3.) ¿Qué posibles soluciones técnicas podrían existir para aplicar modificar o cancelar datos en los bloques?

15. Convendría hacer un breve resumen de consideraciones prácticas asumidas en la investigación de campo cuando se ha realizado consultoría de protección de datos con clientes blockchain reales de ámbito general. Por ejemplo, ¿qué recomendaciones iniciales podríamos dar a los desarrolladores de blockchain en entornos de salud?

Respecto al compliance u responsabilidad en materia de protección de datos para aplicar a la Industria del cuidado de la salud digital.

16. Antes avanzar en este capítulo habría que abordar qué tipos de riesgos posibles con repercusión legal nos encontraríamos en nuestro escenario.

17. Hecho lo anterior, es de gran importancia analizar los *instrumentos* de derecho de protección de datos, al igual que la capacidad para representarse como medio de prueba y evidencia. Por ejemplo, podríamos poner nuestro punto de mira en los *best practices* corporativos o a los códigos de conducta de protección de datos.

18. Investigar cómo surge el *"compliance en protección de datos"* y qué es.

19. Identificar situaciones críticas llamativas donde es clara la responsabilidad de determinados actores: Caso *Boehringuer-Servicios Andaluz y Extremeño de Salud.*

---

ensayos clínicos e investigación científica? ¿seremos capaces de determinar qué tipo de tratamiento de datos se realizan, qué datos hay, qué datos son de carácter personal, y qué sujetos intervienen, etc.? ¿Podremos entender por tanto que una consulta sobre un registro de dato de salud en un sistema blockchain es un tratamiento de datos?

20. Abordar las diferencias entre RSC y ética empresarial, si las hay. ¿De qué forma la tecnología podría ayudar en el ámbito de la responsabilidad y el cumplimiento normativo? ¿Qué tecnología emergente podría ser más conveniente?

21. ¿Cómo es la institución de la indemnización en materia de protección de datos en el marco del régimen sancionador?

Respecto al derecho fundamental de la protección de datos personales. Enfoque desde el ámbito de la Salud y la Tecnología.

22. ¿El derecho a la protección de datos es un derecho humano? ¿ Y fundamental? ¿Y de la personalidad?

23. ¿Se puede comerciar con los datos personales de salud? Sería conveniente extraer situaciones reales donde esto ocurre, por ejemplo, en aseguradoras o en tecnologías blockchain.

Respecto a las cuestiones previas y el nuevo régimen jurídico en materia de protección de datos en Salud y Tecnología.

24. ¿Dónde se concentran los datos de salud en España?, ¿el derecho de los ciudadanos a tener acceso a sus propios datos sanitarios es real? , ¿Qué se podría hacer para conseguir su mayor efectividad?

25. ¿Existen riesgos legales derivados de la reutilización de la información pública?, ¿podríamos considerar a los metadatos como datos personales?

Respecto al nuevo régimen jurídico en materia de protección de datos aplicado del cuidado de la salud digital.

26. En mi humilde opinión, convendría estudiar el alcance y hasta qué punto se podría haber aprovechado la denominada "información por capas" en beneficio del titular de datos antes de la aprobación de la LOPDGDD. (Pienso en *legal design para la comunidad sordomuda en entornos de la Industria de la Salud Digital,* por ejemplo).

27. ¿De qué manera repercute la LOPDGDD en el ámbito de la investigación biomédica?, ¿se otorga mayores protecciones al titular fuente? , ¿Beneficia a la investigación en su conjunto? , ¿O exige más obligaciones a los investigadores?

28. Según el RGPD, ¿cuándo los tratamientos automatizados serán legítimos?, ¿no hubiera sido conveniente que los EEMM regularan o desarrollaran el alcance de las decisiones automatizadas habida cuenta a tecnologías como el *deep learning*, por ejemplo, la intervención humana?

29. ¿Las medidas técnicas y organizativas son obligaciones de medios o de resultados?

30. Estudiar los retos que encuentran ante el Internet del ADN o con la llegada de la computación cuántica en medina respecto a la técnica de la anonimización. Sobre todo, pienso en la anonimización y su eficacia verdadera ante posibles reidentificaciones.

31. Analizar la situación real de las aseguradoras interactivas como responsables del tratamiento de datos cuando se llevan a cabo decisiones automatizadas.

Respecto a las implicaciones éticas desde el punto de vista de la protección de datos y la privacidad en la Industria del cuidado de la salud digital.

32. Analizar los problemas éticos que podrían surgir desde la perspectiva de la investigación científica como bien común. Por ejemplo, pienso en posibles intereses ocultos.

33. ¿Están seguros los ciudadanos, usuarios o titulares de datos con las AAPP de salud? ¿Cómo se podría minimizar los riesgos o posibles vulnerabilidades en los derechos y libertades de las personas?

34. ¿Qué es la ética de los datos? ¿De qué forma podría la ética de los datos solucionar los desafíos que se presentan con la transformación digital de la Industria?

35. ¿Se llevar la ética a las empresas (responsables y encargados de tratamiento) de forma similar a lo que se conoce como RSE empresarial?

36. ¿Cómo será la "ética del futuro" que podremos aplicar a nuestro objeto de estudio?

3.2. Marco metodológico

Respecto a la metodología, en primer lugar, diremos que se ha optado por una *metodología de observación externa* y planificada orientada al fin de la investigación. Como hemos dicho anteriormente, la distinción de los diferentes sectores dentro de la

Industria ha sido importante de cara a la toma de información, análisis y estudio. Como se ha ido señalando a lo largo de los planes de investigación anuales, la asistencia a congresos, seminarios y ponencias ha sido de gran relevancia para generar la perspectiva multidisciplinar que se requiere en la investigación: Derecho, Salud y Tecnología. La mayor labor, posiblemente, ha sido la recopilación de las noticias de actualidad del contexto tecnológico llevado a cabo desde el año 2015 hasta la actualidad. En segundo lugar, hemos de señalar que el *método de análisis de contenido jurídico* se ha completado con sentencias, resoluciones (AEPD), expedientes, y sobre todo, con normas jurídicas, dictámenes, recomendaciones (instituciones comunitarias europeas y autoridades nacionales como el GT29 o el CEPDP). En cambio, el *contenido técnico tecnológico* se ha incluido gracias a papers e investigaciones de investigadores del sector del cloud computing, internet de las cosas, big data e inteligencia artificial, y recientemente añadido en el año 2018, del blockchain o computación cuántica, en el año 2019. Por su parte, el *contenido técnico-sanitario* está incluido por informes y estudios oficiales del ámbito de la e-Health realizado por instituciones públicas europeas o españolas. A su vez, se ha pretendido especial énfasis a la ética de datos, al gobierno corporativo y gestión de riesgos, al compliance, responsabilidad social empresarial, autorregulación, homologación de proveedores en materia de protección de datos, estudiando los sujetos jurídicos implicados bien sea en el contexto de las organizaciones y el sector privado. En tercer lugar, hablaremos del método de las entrevistas, las cuales se han realizado en el marco de foros de expertos e investigadores académicos en universidades. Pero también se han realizado con clientes de mi despacho y profesionales de la tecnología y consultores de gran prestigio. Además, también ha habido entrevistas e intercambio de opiniones con investigadores y profesionales en el marco de asociaciones como la de Quantum World Association) (abril 2019), como hemos citado en párrafos anteriores. Por otro lado, se han iniciado entrevistas en el entorno de la cátedra de Genoma Humano con especialistas y doctores de gran prestigio como D. Iñigo de Miguel (mayo 2019), con quien tengo el privilegio de trabajar como investigadora. Recientemente formo parte de un proyecto de investigación europeo llamado PANELFIT, donde realizamos conversatorio acerca de salud, datos y tecnología.

Por último, destacar las fases temporales que ha requerido el desarrollo del trabajo:

- Fase i. Análisis de la Industria del cuidado de la salud y transformación digital.
- Fase ii. Análisis de las tecnologías aplicadas a las Industria del Cuidado de la Salud digital.
- Fase iii. Análisis y estudio del régimen jurídico de la protección de datos en cloud e IoT en la Industria del cuidado de la salud digital.
- Fase iv. Análisis y estudio del régimen jurídico de la protección de datos en blockchain en la Industria del cuidado de la salud digital.
- Fase v. Estudio acerca del cumplimiento normativo y la responsabilidad adquerida en materia de protección de datos a la hora de aplicarse en la Industria del cuidado de la salud digital.
- Fase vi. Estudio y análisis relacionados con el flujo de datos de salud en el mercado único digital, el open data de salud, la reutilización de datos de la salud, los metadados, etc.
- Fase vii. Análisis del régimen jurídico en materia de protección de datos personales, en concreto, del cuerpo normativo afecto a los datos personales de salud, y específicamente, en el contexto digital.
- Fase viii. Análisis del papel de la ética en este contexto.

5. PRECISIONES TERMINOLÓGICAS Y CONCEPTUALES

En este apartado me gustaría apuntar unas mínimas apreciaciones respecto algunas referencias terminológicas y conceptuales al lector.

Así por ejemplo, en numerosas ocasiones citaré la Industria del Cuidado de la Salud, refiriéndome a la Industria del Cuidado de la Salud "digital" es decir, en el marco de la transformación digital. Al centrar la atención en el ámbito privado, es decir, al sector privado, consideré conveniente utilizar el término "Industria" mejor que otros como "Sector". Por otro lado, conviene destacar las diferentes formar terminológicas que puede adoptar la misma figura jurídica del sujeto "protagonista", es decir, el titular de los datos; "paciente", "usuario", "persona" ,"titular", "consumidor", "persona física", "sujeto", etc. Todas ellas se referirán al titular de datos personales como el poseedor de derechos y libertades. Respecto a conceptos como "dato personal", "tratamiento de

datos personales", "titular de datos" etc., se recomienda al lector, el abordaje del capítulo 4, donde se intentará "desmenuzar" los conceptos más importantes para sentar las bases a la explicación de la nueva normativa. Por otro lado, daré otro apunte, quizás más específico del que no quisiera olvidarme. Me refiero a "blockchain" como "protocolo" más que como "tecnología", per se, no obstante, consideré conveniente referirme a blockchain como ésta último, sobre todo a efectos prácticos, para evitar que el lector pudiera perderse en excesivos purismos conceptuales, olvidando lo realmente esencial, que es, entender a blockchain como una tecnología objeto de estudio. Algo similar ocurre con la referencia de este término cuando en un sentido más purista convendría señalar "DLT" (tecnología de registros distribuidos, en español). Se ha pretendido desde el primer momento hacer fácil la lectura más técnica al lector, no obstante, aprovecho la ocasión para mencionar las diferencias. Una blockchain, es una cadena de bloques y un tipo de DLT. Lo que ocurrió en verdad, fue que el "bombo" o el éxito de este producto o servicio superó el "paraguas" que la engloba que acabó incluso fagocitando su nombre, pero de la misma forma que no todos los correctores de escritura se llaman *"tipex",* no todas las DLT son "blockhain". Para profundizar más sobre ello, recomendamos la lectura del capítulo correspondiente.

Por último, únicamente, me queda anticipar al lector una literatura repleta de tecnicismos –propios de la disciplina de la tecnología - o eventuales referencias médicas o de cuestiones económicas, las cuales procurarán ser lo más claras y sencillas posibles para el público. No podemos olvidar que se trata de un objeto de estudio multidisciplinar: Derecho, Economía, Medicina, Tecnología y Sociología.

CAPÍTULO I. LA INDUSTRIA DEL CUIDADO DE LA SALUD Y TRANSFORMACIÓN DIGITAL.

SUMARIO: 1. INTRODUCCIÓN. 1.1.Los sistemas de salud y el derecho a la salud. 1.2.La Industria del cuidado de la salud. 1.3.Mercado de datos de salud.- 2. EL SECTOR DE LA ATENCIÓN SANITARIA. 2.1.Cambio de paradigma. 2.2.Transformación digital y fuentes de datos. 2.3.Concepto eHealth y tipos. 3. LA INDUSTRIA FARMACÉUTICA DIGITAL.- 3.1.Cambio de paradigma: De Industria tradicional a la tecnológica. 3.2.Transformación digital y fuente de datos. 4. LA INDUSTRIA ASEGURADORA DE LA SALUD DIGITAL. 4.1.Cambio de paradigma y transformación digital. 5. CONCLUSIONES.

"El fundamento de la realidad es el cambio continuo"
Heráclito de Éfeso.

El 54% de los usuarios de Internet están dispuestos a compartir sus datos de salud con el seguro de salud si reciben incentivos. Los científicos esperan que en el 2049 no haga falta acudir al médico, bastando un *selfie* con el teléfono para tener un diagnóstico clínico[8]. El 79% de los usuarios alemanes en línea quieren poder decidir quién puede ver sus datos de salud.

Imaginemos un mundo en donde cada mañana después de levantarnos, acudamos al lavabo para lavarnos los dientes y por medio de nuestro cepillo de dientes inteligente recibamos recomendaciones personalizadas sobre medicamentos y suplementos nutricionales según nuestras necesidades y que, además, analizara *muestras biológicas* periódicamente y ceder (o "alquilar") esa información personal con nuestro consentimiento expreso profesionales de salud investigadores o empresas farmacéuticas[9] como *Bayer o Boehringer* (a través de *smart contracts*, o incluso,

[8]Garcia, L. (20 enero 2018). ¿Cómo diagnosticar enfermedades a través de la forma del rostro?*SaludDigital*. Recuperado de https://www.consalud.es/saludigital/94/como-diagnosticar-enfermedades-a-traves-de-la-forma-del-rostro_45763_102.html

[9] O imaginemos un mundo donde nuestros hospitales y farmacias tienen la ubicación exacta de nuestros dispositivos médicos y la información medico-farmacéutica personal (nombre del médico que nos recetó X medicamento, número de lote, dosis y nombre de medicamentos comprados); y donde las compañías farmacéuticas puedan monitorear los cambios en la demanda en tiempo real y modificar sus cronogramas de producción en consecuencia; y donde los organismos de control (ej. Agencia Española o Europea de

recibiendo una contraprestación o "micropago"). Esto no es imaginación, y puede ser una realidad[10].

Todos ganarían al conseguir un ecosistema de investigación científica mucho mejor. A su vez, la desconexión entre la sanidad pública y la privada es total. Disponer de todos los datos médicos de forma pública, fiable y transparente a la vez que anonimizada permitirá una mayor velocidad y un ahorro de costes en el Sector Público y Privado además de mayor eficiencia al producir mayores soluciones médicas disponibles para el usuario y consumidor.

Dentro de poco, los pacientes[11] en España dispondrán de apps móviles de hospitales públicos y privados, podrán acceder mediante *Blockchain* donde podrán optarán a compartir su información personal con aseguradoras, farmacéuticas, colaborando en investigaciones científicas o ensayos clínicos.

Es claro que todo ello supondrá una auténtica revolución en el uso de los recursos médicos y su gestión.

1. INTRODUCCIÓN

1.1. Los sistemas de salud y el derecho a la salud.

"La salud ya no es solo, como dice la OMS, la ausencia de enfermedad, sino la plenitud en el sentido de que es lo que nos pertenece desde el punto de vista físico, psíquico y social"

(Stefano Rodotà)

Medicamentos o FDA) pueden retirar productos alterados con precisión y velocidad de cada punto en la cadena de abastecimiento. En la actualidad ya hay proyectos en marcha de este tipo. En el campo de la poderosa industria farmacéutica conviene señalar unos datos muy importantes para entender la relevancia de la cuestión; el mercado anual de desarrollo de medicamentos es de 140 mil millones dólares y las compañías farmacéuticas están comprando conjuntos de datos costosos. El coste de los ensayos por paciente es de 36,500 dólares en promedio.

[10]Quijije, J. (17 julio 2017). Crean el primer dispositivo médico en el mundo basado en tecnología Blockchain. *Coincrispy*. Recuperado de https://www.coincrispy.com/2017/07/17/bowhead-dispositivo-blockchain/

[11] Los datos agregados no tienen la calidad de los datos individuales a nivel del paciente que se requieren normalmente. Los pacientes no reciben compensación cuando se venden sus datos agregados y no dan su consentimiento explícito. Blockchain traería beneficios al permitir a las personas que deseen participar en los ensayos agreguen los datos asociados con su salud y hacerlos visibles para todos los reclutadores asociados con las empresas farmacéuticas.

La salud es un estado de completo bienestar físico, mental y social, y no sólo la ausencia de enfermedad (OMS, 1946) y por la propia condición humana, el bienestar es transitorio y difícilmente puede existir un estado de completo del mismo. Desde el punto de vista sociológico, la salud es un proceso donde el individuo tiene un rol activo en el cual intervienen diferentes actores e instituciones como los individuos sanos, pacientes, familia y comunidad, donde además, el papel de prevención, promoción y educación está presente como elementos principales de este proceso (Villareal Valera, 2015)[12]. En ese sentido, *Pierpaolo Donoti*[13] consideraba, que para resolver la crisis del sistema sanitario habría que percibir a la salud como producción de un ambiente sano donde la crisis del sistema sanitario tendría que ser gestionada como "una modificación activa del sistema social en términos de una comunicación auténtica entre instituciones sociales y mundo vital". Los sistemas sanitarios son la suma de todas las organizaciones, instituciones y recursos cuyas actividades están orientadas a mejorar la salud, tanto si éstos son responsabilidad de las AAPP (sector sanitario público)[14] o de empresas privadas (sector sanitario privado)[15] las principales funciones de cualquier sistema deberían ser, según la OMS, "la provisión de servicios, la generación de recursos, la financiación y la gestión".

Y, ¿cómo es la situación de los sistemas de salud en Europa y España? Se tiende a pensar que los sistemas de salud de los países subdesarrollados o en vías de desarrollo son los únicos que presentan deficiencias, sin embargo, la crisis vivida en Europa recientemente ha puesto de manifiesto que la fragilidad del estado de bienestar puede afectar también a los países más desarrollados. En España, por ejemplo, el sistema sanitario se enfrenta a severas dificultades de carácter económico. Según datos recientes del 2015, factores como la inversión en innovación tecnológica y científica**,** *la prolongación de la esperanza de vida, el envejecimiento poblacional o las*

---

[12] Villareal Valera**,** *J.A. (2015). Perspectiva sociológica de la salud como proceso socio cultural. Revista Caribeña de Ciencias Sociales. Recuperado de: http://www.eumed.net/rev/caribe/2015/12/salud.html.*

[13] Donoti, Pierpaolo (1994). Manual de Sociología de la Salud. Ediciones Díaz de Santo, SA. Pp. 30. España.

[14] En el caso de España, el Sistema Nacional de Salud (SNS) se organiza en dos niveles de asistencia: (i) la Atención Primaria, que se centra en abordar los problemas de salud más frecuentes; (ii) la Atención Especializada, que posee medios diagnósticos y terapéuticos más eficientes.

[15] Por su parte, el sector privado está constituido por multitud de empresas que ofrecen a sus clientes productos y servicios sanitarios ajustados a sus necesidades económicas. Piénsese en Sanitas o FIATC o aseguradoras como Adeslas, Axa o Mapfre.

enfermedades crónicas han contribuido considerablemente al crecimiento del gasto sanitario tanto por parte del sector público como del privado. Este hecho ha puesto de manifiesto la necesidad de implementar una serie de restricciones presupuestarias, entre las que se incluyen una importante reducción salarial en el sector hospitalario y un aumento progresivo del precio de los medicamentos.

Pero para hablar de sistemas de salud necesitamos contemplar el *derecho a la protección de la salud,* el cual se incluye en la Constitución Española de 1978 bajo la rúbrica «De los principios rectores de la política social y económica», en el Capítulo III del Título I (art. 43), en los siguientes términos:

> 1. Se reconoce el derecho a la protección de la salud.
> 2. Compete a los poderes públicos organizar y tutelar la salud pública a través de medidas preventivas y de las prestaciones y servicios necesarios. La Ley establecerá los derechos y deberes al respecto.

Es un derecho que se encuadra en los llamados *"derechos sociales de prestación",* cuya característica principal consiste en la implicación de los poderes públicos para su plena realización. Todas las personas tienen derecho a acceder a las acciones sanitarias de tutela de la salud sin necesidad de ostentar ningún título jurídico especial por la sola condición de ser persona[16]. La Constitución Española impone tanto la igualdad jurídica como la igualdad sustancial y para superar las situaciones de desigualdad en la protección de salud de los ciudadanos[17].

1.2. La Industria del cuidado de la salud.

[16] Existen dos clases de derechos de los enfermos: (i) Los sociales, en los que entraría la protección de la salud; (ii) los derechos individuales, en los que estaría el derecho a la utilización de diferentes servicios y prestaciones. Posteriormente se incorporaría el término "paciente" como sustituto habitual del enfermo, más ligado a la terminología hipocrática. (Ver. Leenen, Pinet y Prims, *Trends in Health legislation in Europe.* Masson, 1986).

[17] El Estado goza de las facultades que le concede el artículo 149.1.16 de la Constitución:" El Estado tiene competencia exclusiva sobre las siguientes materias**:** Sanidad exterior. Bases y coordinación general de la sanidad. Legislación sobre productos farmacéuticos."

Según la OMS (1946), la salud es un *estado de completo bienestar físico, mental y social*, y no sólo la ausencia de enfermedad, pero además de esta definición podremos decir que también es un "bien económico" y adquiere una dimensión económica[18].

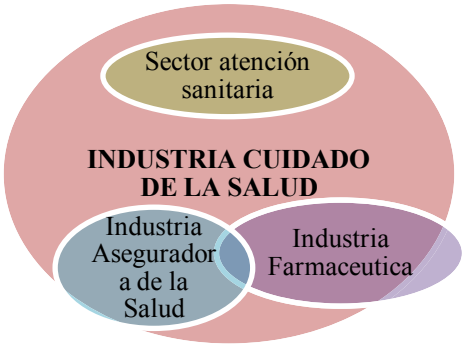


Tabla 1. Esquema gráfico de la Industria del cuidado de la salud.

El *sector salud* es el conjunto de bienes y servicios encaminados a preservar y proteger la salud de las personas. En este sector, profesionales de salud como *médicos y farmacéuticos* prestan los servicios de prescripción médica y específicamente la prescripción de fármacos. Es por ello, que la Industria Farmacéutica puede funcionar. Y además, en este ecosistema se encuentran las *compañías de seguros, las entidades prestadoras de salud y la seguridad social*, las cuales satisfacen la necesidad de tranquilidad ante los riesgos en la salud del paciente/cliente. El envejecimiento de la población y el incremento de la prevalencia de las enfermedades crónicas, y de la dependencia que traen consigo, suponen un cambio de escenario frente a *sistemas sanitarios y de atención social*[19].

---

[18] *Cuando una persona cae enferma o cree que su salud se está deteriorando siente la necesidad de estar sano, pretende mejorar sus condiciones físicas, y además, desea corregir estas situaciones buscado un bien o servicio de salud que le lleve a la recuperación o que al menos mejore sus condiciones. Para satisfacer sus necesidades acude al "mercado" de servicios de salud, donde mediante un pago adquiere un servicio o bien que ayudará a su mejoría de la "depreciación natural". El paciente demandante adquirirá éstos de una forma racional en función del coste, del beneficio que espera recibir y de los incentivos que vaya a recibir de los proveedores de salud (médicos, personal sanitario, establecimientos de salud) para obtenerlos. En este sentido se puede entender que los bienes y servicios de salud son "comercializables" puesto que pueden adquirirse en un mercado bajo las leyes de la oferta y la demanda.*

[19] Ver http://www.fundacioneconomiaysalud.org/wp-content/uploads/2015/07/100-PERSPECTIVAS-PARA-MEJORAR-EL-FUTURO-DEL-SECTOR-SALUD-Fundacion-Economia-y-Salud.pdf. Según la *Fundación Economía y Salud* hay tres hechos relevantes que están marcando las orientaciones estratégicas para mejorar la salud de las poblaciones: "1º) La nueva definición de la OMS del concepto

Dicho esto, y para profundizar y continuar desarrollando ideas sobre la cuestión, partamos del *Esquema mundial de clasificación de la Industria*[20] que hace la siguiente clasificación:

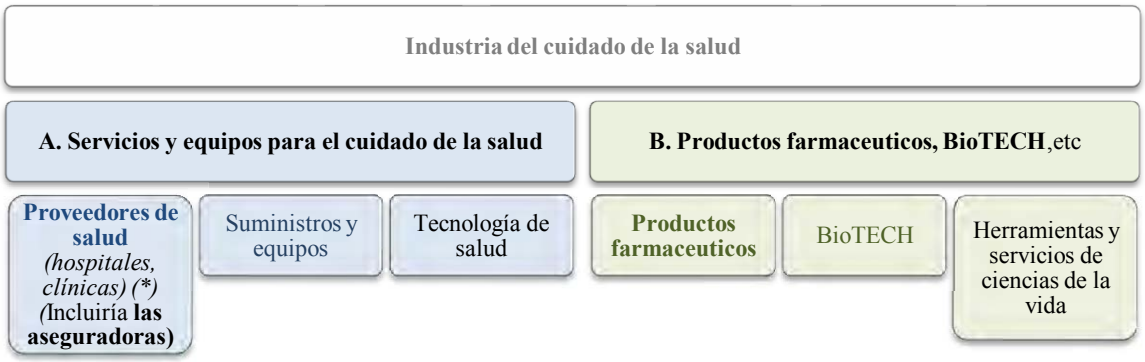


Tabla 2. Industria del cuidado de la salud.

El grupo (azul) de servicios y equipos de atención médica está formado por *compañías y entidades* que proporcionan *equipos médicos, suministros médicos y servicios de atención médica,* como *hospitales, proveedores de atención médica domiciliaria y residencias de ancianos*. El otro grupo (verde) industrial incluye compañías que producen *biotecnología, productos farmacéuticos y servicios científicos diversos.*

A. Servicios y equipos para el cuidado de la salud[21].

i. *Proveedores y profesionales* personal sanitario.

Un proveedor de atención médica es una *institución* (como un hospital o clínica) o una *persona* (como un médico, una enfermera, un profesional de la salud asociado o un trabajador de salud comunitario) que proporciona servicios preventivos, curativos, promocionales, de rehabilitación o cuidados paliativos de manera sistemática

Salud que cambia de "la ausencia de enfermedad" como rasero a superar, al de mayor nivel de autonomía y bienestar alcanzable a conseguir, durante el mayor tiempo posible, aun teniendo enfermedades que aún carecen de curación. Es decir, el objetivo pasaría a ser vivir el mejor estado saludable posible, evitando inicialmente adquirir enfermedades y en su caso.2º) La importancia de la Atención Centrada en la Persona: el concepto global de salud enfocado hacia el bienestar y autonomía. 3º) La atención holística de las necesidades de las personas, sólo será posible desde una atención multidisciplinar, intersectorial y coordinada. El hospital centrismo, la descoordinación entre niveles asistenciales y sectores, así como una oferta de servicios no unida a su rendimiento en resultados reales sobre la salud de la población, requiere un giro urgente."

[20] Ver https://www.msci.com/www/research-paper/the-new-gics-communication/01107886967

[21] También incluye otras acciones clave relacionadas con la salud, como la educación y capacitación de profesionales de la salud, la regulación y gestión de la prestación de servicios de salud, el suministro de medicamentos tradicionales y complementarios, y administración de seguros de salud.

para individuos, familias o comunidades. La industria de la salud es uno de los segmentos más grandes de la fuerza laboral[22]. Se espera que la participación en la salud del producto interior bruto (PIB) continúe su tendencia al alza, alcanzando el 19,9 por ciento del PIB en 2025. en España (2014) le correspondía un 9,1 % frente al 11% de Alemania o el 16,6 % de USA o el 11,4 % de Japón.

Gasto sanitario público y privado como porcentaje del PIB a precios de me
1980-2014

País	1980	1990	2000	2013	2014
Austria	7,0	7,7	9,2	10,1	10,3
Belgium	6,1	7,1	7,9	10,4	10,4
Czech Republic	-	3,8	5,7	7,8	7,7
Denmark	8,4	8,0	8,1	10,3	10,6
Estonia	-	-	5,2	6,0	6,1
Finland	5,9	7,2	6,9	9,5	9,5
France	6,7	8,0	9,5	10,9	11,1
Germany	8,1	8,0	9,8	10,9	11,0
Greece	-	6,1	7,2	8,7	8,3
Hungary	-	-	6,8	7,3	7,2
Iceland	5,9	7,4	9,0	8,8	8,9
Ireland	7,5	5,6	5,9	10,5	10,1
Italy	-	7,0	7,6	8,8	9,1
Luxembourg	-	-	5,9	6,5	6,3
Netherlands	6,6	7,1	7,1	10,9	10,9
Norway	5,4	7,1	7,7	8,9	9,3
Poland	-	4,3	5,3	6,5	6,4
Portugal	4,8	5,5	8,4	9,1	9,0
Slovakia	-	-	5,3	7,6	7,0
Slovenia	-	-	8,1	8,8	8,5
Spain	5,0	6,1	6,8	9,0	9,1
Sweden	-	7,3	7,4	11,1	11,2
Switzerland	6,6	7,4	9,3	11,2	11,4
Turkey	2,4	2,5	4,7	5,1	5,1
United Kingdom	5,1	5,1	6,3	9,9	9,9
Europe	6,1	6,4	7,2	8,7	8,8
USA	8,2	11,3	12,5	16,4	16,6
Japan	6,4	5,8	7,4	11,3	11,4

Nota: Europa: promedio no ponderado (25 países) - cálculos EFPIA

Imagen 1. Gasto sanitario público y privado como % del PIB. Fuente: Pharmaceutical Executive

ii. Prestación de servicios.

Hay muchas formas de brindar atención médica en el mundo moderno. El lugar de entrega puede ser en el hogar, la comunidad, el lugar de trabajo o en instalaciones de salud. La forma más común es la forma presencial (*face to face*) donde el proveedor de atención y el paciente se ven en persona, sin embargo, con la tecnología y la digitalización llegan otras formas de prestación de servicios como la telemedicina. Según *PwC*[23], el mercado sanitario global *conectado* vale 61 mil millones de dólares en 2020 con una tasa de crecimiento anual del 33% . En concreto, el mercado

[22] Ver https://www.who.int/whosis/whostat/ES_WHS2011_Full.pdf?ua=1 Pp. 115 y ss. (última fecha consulta 26.12.2018). Además, según la OMS se estima que hay una escasez mundial de alrededor de 4,3 millones de médicos, enfermeras y trabajadores de la salud aliados. Con las enfermedades de la era moderna como la diabetes y la obesidad en aumento, se espera que los costes de atención médica crezcan aún más rápido.

[23] Ash, S. (25 de mayo de 2016). The value of patient data. *Pwc Uk Blogs*. Recuperado en https://pwc.blogs.com/health_matters/2016/05/the-value-of-patient-data.html

de la salud digital global tiene un valor de 536 mil millones de dólares en 2025 según *Transparency Market Research*[24].

B. Productos farmacéuticos, biotecnología y ciencias de la vida relacionadas: ***Industria Farmacéutica.***

Por otra parte, el sector salud posee una vertiente empresarial que se dedica a la fabricación, preparación y comercialización de productos farmacéuticos para el tratamiento y la prevención de enfermedades, conocida como la Industria Farmacéutica[25]. Éste es uno de los sectores económicos más importantes del mundo. Por cada dólar invertido en fabricar un medicamento se obtienen mil de ganancias. El sector farmacéutico se encuentra en continuo crecimiento y se caracteriza por una competencia oligopólica en la que 25 empresas controlan cerca del 50% del mercado mundial. La colaboración de las multinacionales farmacéuticas con la industria química, las universidades, y su apuesta en el I+D han ayudado al crecimiento económico y al desarrollo de la ciencia y la tecnología. Por otro lado, la innovación tecnológica de la *secuenciación del ADN y la biotecnología* favorecerán la aparición de nuevos fármacos que antes eran difíciles o imposibles de producir. Pero hay que ser realistas, no toda la población podrá acceder a esos fármacos. Según *Pharmaceutical Executive*[26] (2016), en el ranking de laboratorios por ventas a nivel mundial se

[24] Transparency Market Research (2018). Global Digital Health Market. Recuperado en https://www.transparencymarketresearch.com/digital-health-market.html

[25] Abarca la biología, bioquímica, ingeniería, microbiología, farmacia y farmacología, medicina, enfermería, física, etc. Esta industria desarrolla actividades de investigación y desarrollo (I+D), producción, control de calidad, marketing, representación médica, relaciones públicas o administración.

[26] Aunque no es temática de este trabajo conviene conocer algunos datos de interés respecto a esta industria para comprender el interés que despiertan los datos de salud (y personales) extraídos en el marco de los gigantes farmacéuticos. Las estrategias "no muy legítimas" de esta industria se refieren a: (i) *Estrategias respecto a las patentes comerciales.* Mucho tiene que ver la ley de extensión de patentes aprobada en 1984 cuando hasta esa fecha la política de patentes no afectaba a los medicamentos por considerarlos un bien necesario. "Ahora, el 60% de las patentes de medicamentos son de EE.UU., frente al 20% de la Unión Europea. Gracias a esto EE.UU. domina el mercado de los 50 medicamentos más vendidos y su elevado coste que es fijado abusivamente por los laboratorios"."El principal argumento para mantener las patentes de los medicamentos esta en los gastos por investigar nuevos medicamentos, sin embargo la mayor parte del coste de la investigación de un nuevo fármaco no recae sobre la industria ya que los gobiernos y los consumidores financian el 84% de la investigación, mientras que solo el 12% correspondería a los laboratorios farmacéuticos." (ii) *Estrategias incrementando el precio de medicamentos.* El incremento de los costes no está relacionado con la fabricación de los medicamentos, ni tampoco con la inversión en investigación y desarrollo, sino en los gastos asociados a la comercialización y la promoción de sus productos. Los costes de producción se han visto reducido gracias a la automatización de dicha producción. Mas bien, los costes proceden como consecuencia de la realización de estudios de mercado, análisis de competidores, extensión de patentes, distribución, promoción, publicidad y ventas de sus productos, gastos administrativos para mantener estructuras multinacionales y

encuentran en eses orden: *Pfizer, Novartis, Roche, Merck % Co, Sanofi , Johnsons & Johnson, Gilead, GSK, Abbvie y Amgen*. En nuestro país, esta industria genera un gran volumen de ventas y posee una de las mayores tasas de productividad a nivel mundial[27]. Por su parte, la inversión en investigación y desarrollo de la industria asentada en España alcanzó cifras altas[28]. En *Farmaindustria*, consideran que "este esfuerzo junto con la estrecha colaboración con la Administración y los centros sanitarios y de investigación, la implicación de los profesionales sanitarios y la *creciente participación de los pacientes,* ha permitido situar a España como uno de los países europeos con mejores condiciones para albergar *ensayos clínicos*[29], hasta el punto de que un tercio de todos los realizados en Europa cuentan ya con participación española. Incluso, para algunas compañías multinacionales, España es el segundo país, tras EEUU, en participación en *ensayos*".

---

los astronómicos salarios pagados a sus ejecutivos. Actualmente la compañía farmacéutica Gilead está ganando ingentes beneficios gracias al tratamiento contra la hepatitis C, sofosbuvir al que al parecer puso el astronómico precio en España de 25.000 euros (80.000 dólares en USA) . (iii) *Estrategias donde se actúa con poca transparencia.* En algunos casos se "maquillan" los ensayos clínicos para mejorar sus resultados e incluso se ocultan efectos adversos. (iv) *Estrategias para incrementar la venta.* Cada vez los gobiernos reducen el gasto farmacéutico (25-30 % del gasto sanitario total) y para compensar esta situación los laboratorios en algunas ocasiones; promueven el tratamiento de problemas leves o de mediana gravedad, estimular la preocupación sobre futuras enfermedades como el alzhéimer o los trastornos de ansiedad, o considerar ciertas enfermedades como epidemias de extraordinaria propagación o letalidad como la gripe A. Algunos laboratorios organizan congresos con asociación de enfermos para presionar a los gobiernos y de esta manera obtener fármacos aunque no esté justificada su necesidad o tengan efectos adversos. Vid. Federación de Asociaciones para la Defensa de la Sanidad Pública (19 agosto 2017). La enfermedad, un negocio para la industria farmacéutica. *Nueva Tribuna.es*. Recuperado en https://www.nuevatribuna.es/articulo/sanidad/enfermedad-negocio-industria-farmaceutica/20150302105350113131.html

[27] Según el informe *"la farmacia española, en cifras"*, las oficinas de farmacia españolas facturaron 19.337,4 millones de euros entre los meses de mayo de 2017 y abril de 2018. En concreto, el mercado farmacéutico ha *crecido un 1,3% en facturación*. En relación con la cuota de mercado en España, los 10 laboratorios que lideran son *Gsk España, Laboratorios CINFA, Boehringer Ingelheim España, Sanofi España, MSD, Novartis, Pfizer, AstraZeneca Farmacéutica Spain, Bayer Hispania y Janssen-Cilag* en décima posición. Vid. https://www.imfarmacias.es/noticia/15355/el-mercado-farmaceutico-crece-un-13-en-facturacion

[28] En concreto, alcanzó los 1.147 millones de euros en 2017, lo que supone un aumento del 5,7% respecto al año anterior, recoge la *Encuesta sobre actividades de I+D* publicada recientemente por la patronal Farmaindustria. España se ha convertido en una potencia en *ensayos clínicos* y los datos recién publicados constatan esta tendencia al alza. De los 1.147 millones invertidos en I+D en 2017 por la industria farmacéutica, cerca del 60% se dedicó a *ensayos clínicos.* Las inversiones en fases tempranas (I y II), "que son las que requiere de un mayor nivel de complejidad", adquieren protagonismo y hoy representan el 36% del total de la investigación clínica. Mientras que los ensayos de fase III, "que compraran la seguridad y eficacia del nuevo tratamiento con la del fármaco de referencia vigente, suponen el 54,6% del total. Esta actividad ha crecido a un ritmo del 4,9 en los últimos 10 años, al pasar de los 412 millones en 2007 a 662 en 2017.

[29] Simón Ruiz, A. (28 de junio de 2018). Los pagos de las farmacéuticas a los médicos se disparan un 12% hasta 564 millones. *CincoDías*. Recuperado en https://cincodias.elpais.com/cincodias/2018/06/28/companias/1530186688_725021.html

1.3. Mercado de datos de salud.

Según la Comisión Europea[30] , el mercado global de los datos médicos; "se estima que el mercado global de datos médicos valdrá $ 14 mil millones en 2017, y se proyecta que llegará a $ 69 mil millones para 2025, impulsado por una mayor adopción de almacenamiento en la nube, iniciativas gubernamentales a gran escala y una creciente demanda de dispositivos portátiles. Con respecto a esto último, *McKinsey* estima que para el año 2025, alrededor de 1.3 mil millones de monitores de estado físico estarán en uso en todo el mundo. Los inversionistas en el cuidado de la salud en el futuro o las oportunidades digitales de salud no necesitan buscar más."

Ahora bien, *¿cuánto valen los datos de salud?* IBM compró *Truven Health Análisis* por $ 2.6 mil millones para capacitar a Watson en 200 millones de registros de pacientes[31], lo que significa que un registro equivaldría a *13 dólares.* En algunos estudios[32], el precio por conjunto de datos de pacientes puede exceder de 24.600 euros. Se habla de un promedio de *441 euros por paciente* pagados al médico que proporciona los datos. Pero recopilar los datos de los participantes y profesionales de salud tiene un coste no sólo por el proceso en sí, sino también por la propia estandarización y refinamiento cuyo labor dependería de los intermediarios que organizan la población de estudio y los auditores. *¿Por qué es ventajoso este mercado para la Industria farmacéutica?* La existencia de un buscador de datos puede ahorrar en el reclutamiento

---

[30] Comisión Europea (6 de junio de 2017). *European Data Market SMART 2013/0063 Final Report*. Recuperado en https://ec.europa.eu/digital-single-market/en/news/european-data-market-study-data-related-health-tech-growing-fast. La CE también señala que "El valor de la economía europea de datos fue de 300 000 millones de euros en 2016. Si se aplican las medidas legislativas y políticas adecuadas, este valor podría aumentar hasta los 739 000 millones de euros para 2020, el 4% del PIB de la UE . En la UE, la reutilización de datos generados por organismos del sector público (por ejemplo, legal, de tráfico, meteorológico y financiero, etc.) con fines comerciales y no comerciales se rige por la Directiva 2003/98 / CE sobre la reutilización de la información del sector público . En 2012, la Comisión adoptó un paquete de políticas que contiene una serie de medidas para mejorar el acceso a la información científica en Europa, incluida la Recomendación sobre el acceso y la preservación de la información científica resultante de la financiación pública. Entre enero y junio de 2017, la Comisión mantuvo un diálogo con las partes interesadas sobre la Comunicación sobre la construcción de una economía europea de datos., encontrando un fuerte apoyo a las medidas no regulatorias para maximizar y organizar el acceso y reutilización de datos en contextos de empresa a empresa. ".

[31] EFE Nueva York (18 de febrero de 2016). Ibm desembolsará 2.300 millones por la empresa de datos Truven Health Analytics. *Expansión.* (Recuperado en http://www.expansion.com/empresas/tecnologia/2016/02/18/56c5eae5268e3ed4668b46b1.html

[32] Spelsberg A., Prugger C., Doshi P., Ostrowski K., Witte T., Hüsgen D. et al. (7 de febrero de 2017), Contribution of industry funded post-marketing studies to drug safety: survey of notifications submitted to regulatory agencies . *The bmj*. Recueperado en https://www.bmj.com/content/356/bmj.j337

de participantes con los requisitos necesarios y que estén dispuestos a proporcionarlos. Esta reducción de tiempos para las organizaciones de comercialización otorgaría enormes beneficios a los pacientes, la industria y sistemas de salud. En este punto, la tecnología *Blockchain* -de la que hablaremos en el capítulo correspondiente- tiene mucho que decir.

2. EL SECTOR DE LA ATENCIÓN SANITARIA

2.1. Cambio de paradigma

En el futuro los mejores hospitales estarán en Internet y la información genética invadirá el *cloud,* convirtiéndose en el "*cloud* médico" o el "*cloud* genético" El e-paciente se empodera y tendrá mayor acceso a la información médica personal.

Imagen 2. Hospital del futuro. Fuente: Blog Bankinter

La tecnología 5G permitirá varias cuestiones[33]: (i) poder descargar mayores volúmenes de datos importantes en la gestión hospitalaria, análisis de datos o robótica sanitaria y (ii) la velocidad en el acceso a las aplicaciones será mayor en los entornos hospitalarios, por ejemplo. Es decir, toda una revolución en el ámbito de la cirugía a distancia, videoconferencias y tele consultas con calidad, formación on-line en directo. Pero el camino no ha sido corto. Además, blockchain en la atención sanitaria tendrá un

[33] Vid. https://www.redaccionmedica.com/secciones/tecnologia/el-5g-llega-a-espana-asi-revolucionara-y-pondra-en-peligro-a-la-sanidad-3139

papel importante[34] y una repercusión económica en el mercado sanitario: 7.790 millones de dólares en 2027 [35].

A lo largo de la historia se ha pensado siempre que el enfermo está incapacitado desde el punto de vista biológico porque la enfermedad le ponía en una situación de sufrimiento, invalidez y de dependencia. La relación médica paternalista estaba formulada por el juramento hipocrático en la que se establecía una relación vertical y asimétrica en la que "el médico era como un padre benévolo y el paciente se dejaba llevar como un niño sumiso" (Lázaro y Gracia, 2016) [36]. Al igual que las revoluciones liberales lograron emancipar a los ciudadanos del absolutismo y les proporcionaron los derechos civiles y políticos; una revolución particular y un conjunto de factores sociales, clínicos, políticos y científicos se inmiscuyeron en la tradicional relación entre médico y paciente que existía desde la antigüedad (Gómez Ullarte, 2014) [37]. Es evidente que cualquier cambio acarrearía incertidumbres para todos los agentes que interactúan en torno a él. En 1973, se produce la rebelión de los pacientes con la llegada de la primera Carta de Derechos del Paciente que supone el reconocimiento oficial del derecho del enfermo a recibir una completa información sobre su situación clínica y a decidir entre las opciones posibles, como adulto autónomo y libre. A partir de este momento, el enfermo deja de ser paciente –es decir, *pasivo*- para convertirse en *agente*. Desde los inicios de la medicina, los médicos han intentado tomar decisiones informadas con un conjunto muy limitado de herramientas y una cantidad creciente de experiencia que podría transmitirse a la próxima generación[38]. Es finalmente adentrado el siglo XX cuando el paciente pidió que su subjetividad fuera atendida por el médico. La forma en que se concretó la respuesta médica a esta demanda fue la del

[34]Vid. https://www.technologyreview.es/s/9551/blockchain-promete-acabar-con-el-descontrol-y-la-ineficiencia-de-datos-sanitarios-del-mundo

[35] Vid. https://www.ituser.es/actualidad/2019/07/blockchain-en-el-mercado-sanitario-alcanzara-un-valor-de-casi-7790-millones-de-dolares-en-2027

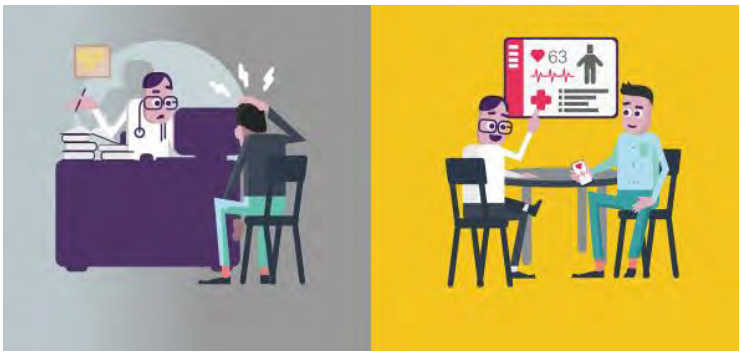
[36] Lázaro, J, Gracia, D. (2006). La relación médico-enfermo a través de la historia. *Anales del Sistema Sanitario de Navarra*. Vol. 29, supl.3. Pamplona. Recuperado en http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1137-66272006000600002

[37] Gómez-Ullarte Rasines, Susana (2014). Historia de los derechos de los pacientes. *Revista de Derecho UNED*, núm. 15.

[38] Incluso en el caso del primer estetoscopio, un tubo de madera hueco introducido por el *Dr. Laennec* en Francia a principios del siglo XIX. llevó décadas difundir la idea de mejorar la atención con una innovación. Desde entonces, la atención de la salud se ha vuelto dependiente de las tecnologías. Los modelos de sistemas sanitarios europeos; -en primer lugar, el de *Bismark* introducido en 1883 financiado por las cotizaciones sociales obligatorias y el *Beveridge* que apareció en 1943 soportado por los impuestos generales- perseguían la bondad del sistema, independiente del resultado final, es decir, hubiera curación o no. Estos permitieron el acceso universal, incrementó la esperanza de vida y mejoró los hábitos de vida saludable, pero se trataba de un contrato social de "medios" y no de resultados.

consentimiento informado[39]. Esta revolución vino acompañada del cambio de rol del médico, la pérdida de su impunidad, la especialización, la estructuración en 3 niveles (primario, secundario con los ambulatorios, y terciario con los centros hospitalarios). No sólo la relación médico-paciente se ha visto modificada en las últimas décadas sino que la propia medicina está en continua evolución. Autores pertenecientes a la *University Singularity* [40]que defienden la teoría de la exponencialidad declaran que, valga la redundancia, esa evolución es exponencial. Sostienen que el futuro de la medicina pasa por ser una medicina digital, personalizada, continua, cuantificable y predictiva.

El modelo paternalista de la relación médico-paciente ha comenzado a ser reemplazado por una toma de decisiones compartida en la segunda mitad del siglo XX[41]. En el Siglo XXI, la situación se hace insostenible debido al aumento de población, la cronicidad de las enfermedades o al incremento del precio de la tecnología. El modelo "industrial" de acceso a la salud empezó a cuestionarse para cambiar a un *modelo asistencial* basado en el valor. Respecto a la relación médico-paciente, nos encontramos en un proceso de evolución de *la medicina paternalista a la medicina digital.*



[39] Castellano Arroyo, M (1944). El consentimiento informado de los pacientes. *Manual de bioética general.* Ed. Dr. Aquilino Polaino-Lorente. Madrid.
El autor señala algo que se podría extender a nuestra materia jurídica de protección de datos; "el mejor conocimiento mutuo crea en el paciente la conciencia de que se le ha tratado lealmente, lo que puede hacer que desista de interponer una demanda si surgen problemas", ya lo que en sí molesta, es el sentirse menospreciado más que la valoración concreta del daño real.
[40] Ver Web de Singularity University; https://su.org/
[41] Según el sociólogo *Parson*, el sistema sanitario debería ser planteado como "un medio generalizado de comunicación y de intercambio, entre individuos, sistemas y ambiente". Por su parte, *Donati* (1994) criticaba a la corriente funcionalista que no se reconocía la posibilidad de expresarse a través de precisos canales de comunicación y de *feedback* en el sistema social". Era necesario expresar claramente la importancia de la participación activa de los pacientes. En este sentido, Habermas defenderá la necesidad de una nueva forma de democracia basada en la participación donde el elemento fundamental sea el consenso y todos participemos en el mismo nivel de importancia.

Imagen 3. Diferencias entre consulta del presente y del futuro. Fuente: mHealthsgroups

En el pasado, los médicos actuaban guardando la información médica privada comunicando los resultados a los pacientes siempre que fuera necesario, ahora, la información es un arma muy poderosa para capacitar a los ciudadanos en la toma de decisiones sobre todo aquello que afecta a su salud. En el siglo XXI aparece el concepto *"alfabetización de salud"* como la capacidad para acceder a la información, interpretar y juzgarla adecuadamente y aprovecharla para tomar decisiones adecuadas sobre nuestra propia salud. En España parece haber un problema, precisamente sobre alfabetización de la salud, así lo dicen los estudios. Según la ONTSI, el 62% de los pacientes asegura no disponer del conocimiento necesario sobre su enfermedad (ONTSI, 2016) y que la mayoría de las personas que salen de una consulta indican que la información escrita proporcionada por los profesionales resulta difícil de comprender y no está adaptada al usuario al que se dirige (Mayor Serrano, 2010)[42].

Si pensamos en las enfermedades crónicas, o trastornos psiquiátricos los pacientes no adquieren esa información. Los profesionales atienden a más pacientes en menos tiempo y con mucha carga administrativa. Estamos avanzamos hacia la *"medicina 4p"* (preventiva, poblacional, proactiva y participativa) del científico norteamericano *Leroy Hood*[43]. Ya el *Dr. Tom Ferguson* acuñó el término *e-patient*[44] y su conciencia comenzó a aumentar alrededor de 2009. Otorgar cierta tecnología disruptiva a un paciente no ha mejorado por sí solo los resultados de salud, sino van acompañados del factor humano implicando al paciente con retroalimentación y recompensas por el esfuerzo.

Para el *Dr. Meskó Bertalan*[45], doctor futurista y genomista, los grandes cambios de la medicina del futuro podrían ser los cuatro siguientes:

i. *Adoptar tecnologías médicas disruptivas.* Según el Doctor, la tecnología médica tiene décadas de antigüedad y está obsoleta, por ejemplo, piénsese en el estetoscopio que tiene más de 150 años, el tensiómetro que tiene 135 años o incluso el desfibrador con 70 años. Ahora, por

[42] Mayor Serrano, B. (2010). Alfabetización en salud.
[43] Hood L. (2013). Systems Biology and P4 Medicine: Past, Present, and Future. Rambam Maimonides Med J.
[44] Fox S. (2008). The Engaged E-patient Population. Pew Internet Am Life 1-4.
[45] Ver página web The Medical Futuristic Institute (Dr. Meskò Bartalan). Recuperado en http://tmfinstitute.org/

ejemplo, este estetoscopio[46] permite visualizar al tiempo real los sonidos cardiacos y pulmonares a través del *Smartphone*[47]*:*

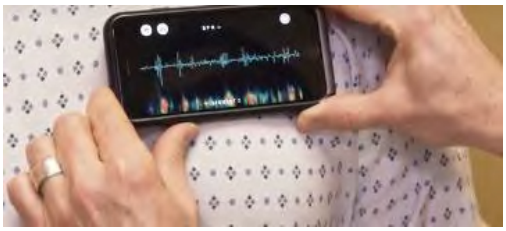


Imagen 4. Estetoscopio y smartphones. Fuente: Steth IO.

ii. *Poner a los pacientes en el centro de la atención médica.* Los pacientes deben convertirse en expertos acerca de su propia salud para poder participar en el diseño de la atención médica. Pero aunque hay una gran cantidad de información disponible en línea, gran parte de ella es parcial o defectuosa.

iii. *Digitalizar información de atención médica.* La digitalización puede hacer que los cuidados sean asequibles y estén disponibles, asegurando la sostenibilidad y aumentando la comprensión de las enfermedades a los usuario.

iv. *Cambiar el enfoque del tratamiento a la prevención*. **Se puede lograr debido a los nuevos wearables y otros sensores** portátiles, ingeridles y digeribles que brindan acceso a datos en tiempo real ayudando a comprender su salud y a modificar comportamientos. Pero no todos los profesionales de salud están capacitados para entender de tecnología[48]. Por ejemplo, *Apple HealthKit* permite transmitir un registro médico electrónico –con datos como el peso, calorías y ritmo cardíaco- a la Universidad de Standford para su investigación[49]. Hoy en día se puede recibir el *feedback* del médico de atención primaria respecto a esos datos recogidos[50].

[46]Redacción Consalud (15 de mayo de 2018). Un nuevo estetoscopio revoluciona el uso de los teléfonos inteligentes.*Consalud.es*.Recuperado en https://www.consalud.es/tecnologia/nuevo-estetoscopio-revoluciona-el-uso-de-los-telefonos-inteligentes_50170_102_amp.html

[47] El *Dr. Meskó Bartalán* añade algo muy importante, y es que para adoptar las tecnologías médicas disruptivas serían necesarios tres pasos: en primer lugar, mejorar la capacitación médica y alfabetización digital de salud para preparar a la nueva generación de médicos. Es importante que los médicos sepan como interactuar con los pacientes a través de las redes sociales. En segundo lugar, se debe educar a los pacientes para que aprovechen las tecnologías. En tercer lugar, los reguladores deben entender los cambios venideros. La ley GINA (ley de no discriminación por información genética en EEUU) protegería los datos confidenciales de los pacientes, donde sería conveniente, por ejemplo, organizar un consejo asesor de pacientes.

[48]Incluso las medidas preventivas simples como el uso diario de aspirina, el apoyo para dejar de fumar y las pruebas de detección de abuso de alcohol pueden salvar 2 millones de vidas y casi $ 4 mil millones anuales.

[49]Ver web *Apple Researchkit* en https://developer.apple.com/researchkit/

[50] Siwicki, B. (2 de octubre de 2017). "Traiga sus propios datos" en la próxima tendencia en salud. *Healthcare IT News.* Recuperado en http://www.healthcareitnews.com/news/bring-your-own-data-next-trend-healthcare

Cabe añadir que la medicina también será *personalizada* o genómica otorgando el tratamiento adecuado al paciente por medio de la observación de los pacientes como si se tratara de un "traje a medida" Pero también será *participativa* donde población enferma como de la saludable a partir de información creada "voluntariamente" a través de dispositivos, sensores, redes sociales, etc.

La *atención sanitaria digital* no sustituye a la atención convencional sino que complementa y mejora al rendimiento de un paciente posibilitando que hospitales ofrezcan contenidos de salud online de cada enfermedad o dolencia. El *sector de la Salud* no sólo se ha ido informatizando en el ámbito público como privado, prueba de ello son la cita sanitaria multicanal, el historial clínico electrónico (HCE), la telemedicina o tele consulta, la receta electrónica, el portal virtual del cliente etc. como veremos en este capítulo sino que paralelamente se han ido implementando las tecnologías del IoTH, *cloud computing*, inteligencia artificial, impresión 3D, realidad virtual entre tantos, sin olvidar la movilidad y las redes Wifi.

Imagen 5. Presente y futuro de la Industria del cuidado de la salud y la tecnología. Fuente: Accenture[51].

Por otro lado, el paradigma tecnológico y social cambia y paralelamente, también lo hace el modelo de negocio de la sanidad: nos dirigimos a la *"sanidad con valor"*. El ecosistema sanitario necesita mejorar la eficiencia y la calidad en los servicios y atención sanitaria, de tal forma, que las inversiones se dirijan a conseguir mejores

[51]Recuperado en https://www.accenture.com/t20150914T131203__w__/us-en/_acnmedia/Accenture/Conversion-Assets/Microsites/Documents20/Accenture-Healthcare-Technology-Vision-2015-Infographic.pdf

resultados en salud de las personas[52]. Pero, ¿por qué es importante una mayor rentabilidad del gasto sanitario? Como sabemos el gasto en salud mundial es insostenible, como ilustra un estudio de Foro Económico Mundial vamos a gastar 47 billones de dólares en enfermedades crónicas en diez años, las cuales suman el 75% del coste total sanitario. Este podría ser el reto que deberá afrontar la salud digital. La inversión en sanidad por parte del enfermo crónico es para toda la vida (OMS, [53]. El economista conductual y director de EY, *Gautam Jaggi* señala que es posible que la tendencia sea que la financiación se apoye entre varios agentes donde se compartan beneficios y riesgos a largo plazo [54].

2.2. Transformación digital y fuentes de datos.

Según el vicepresidente y de la Comisión Europea y responsable del Mercado único Digital, *Andrus Ansip*[55]*dijo*;

> "Los dispositivos como teléfonos inteligentes, tabletas y sensores inalámbricos que se pueden usar en salud móvil, o mHealth , son ahora mucho más accesibles y fáciles de usar. .."

Además, añade:

> "Los análisis de datos avanzados permiten acelerar la investigación y el desarrollo de nuevos tratamientos y mejorar la prevención y detección temprana de enfermedades. Europa está avanzando mucho en esta área, pero no lo suficiente. *Tampoco hacemos el mejor uso de los registros de salud y conjuntos de datos existentes*. Estos no se gestionan por igual en todos los países de la UE o en los sistemas sanitarios nacionales. A menudo, no están disponibles para las autoridades públicas, profesionales médicos e investigadores para ayudarles a desarrollar y proporcionar un mejor diagnóstico. Y con demasiada frecuencia, los conjuntos de datos ni siquiera están disponibles para los pacientes afectados. No debería ser así."

---

[52] Muir Gray, J.A. (2011). *How to Get Better Value Healthcare*. Offox. Edic sec. (Para este autor es necesario pasar de una asistencia de bajo valor, basada en la burocracia, a una asistencia de alto valor, que ha de ser personalizada y basada en las necesidades del conjunto de la población. La democratización de la información ha llegado para quedarse a través de la revolución tecnológica que supone internet y las nuevas herramientas asociadas).

[53]Organización Mundial de la Salud (OMS) . *Preventing chronic diseases: a vital investment*. Recuperado en http://apps.who.int/iris/bitstream/10665/43314/1/9241563001_eng.pdf

[54]Vid en https://www.fundacionbankinter.org/documents/20183/97216/Salud++Digital+ES/5f5bd348-ca10-49de-8bfe-2ba368a2e269 . Pág. 40.

[55] Andrus Ansip; Comisión Europea (20 de abril de 2018). Making digital technology work for healthy livind. *Blog Post European Commission*. Recuperado en https://ec.europa.eu/commission/commissioners/2014-2019/ansip/blog/making-digital-technology-work-healthy-living_en

"Digital" significa usar tecnología, almacenar y procesar los datos. La Salud Digital no es un fin en sí mismo, sino una herramienta que puede dar respuesta a algunas de las necesidades imperiosas de los sistemas sanitarios. Los representantes de los colectivos más implicados en la transformación digital en el Foro *Future Trends Forum* establecieron los beneficios[56]. Además, se podrán estandarizar los cuidados en salud a nivel mundial cerrando la brecha de la desigualdad y garantizando un modo de vida saludable. También permitirá a las personas ser más conscientes sobre su estado de salud y les motivará a modificar sus comportamientos para mejorarla. En el Foro, también se trataron de identificar las mayores barreras, centrándose en que:

i. Los *organismos públicos sanitarios* encuentran *barreras políticas* en el ciclo de campañas electorales y el personal de las instituciones no cuentan con incentivos para innovar[57].
ii. Los *pacientes* tienen cierta inseguridad respecto al *uso indebido de los datos de los pacientes.* Por otro lado, tienen un exceso de información que necesitan "entender" e interpretar de una manera correcta. También podrían ser los encargados de liderar esta barrera exigiendo una mejora en el acceso a la información sobre su historial médico y su enfermedad.
iii. Los *profesionales de la salud* tienen problemas de comunicación interdepartamental puesto que fluye por medio de sistemas de información sanitaria está basado en silos.

Por el momento la llegada de la transformación digital[58] está siendo "escurridiza" puesto que los consumidores de salud digital o *e-Health* no sienten conformidad con pagar y los proveedores de salud son aún escépticos al no existir evidencias consolidadas. No obstante, por muy escurridiza que sea debemos estar atentos a la protección de los datos personales de salud implicados en el proceso de transformación digital.

[56] Vid. Informe Bankinter Pag. 50.
[57] Tampoco existen estándares ni un marco normativo suficientemente fuerte como para armonizar la digitalización del sistema. Se necesita un consorcio interdisciplinar donde estén integrados todos los actores del sistema para desarrollar estrategias políticas y marcos regulatorios que favorezcan la implementación de la Salud Digital y que además estas estrategias estén coordinadas por líderes locales adecuándolas a la casuística de cada región.
[58] Según Julio Mayol (2017) la transformación digital se conseguirá a través de la innovación social, de negocio y tecnológica. Respecto a la transformación social se deberán tener en cuenta tres factores del sistema: (i) las personas: tecnologías para la formación, el entrenamiento y la ayuda a la toma de decisiones; (ii) los recursos materiales: sistemas con automatización y robotización de procesos; (iii) las reglas de funcionamiento: incluye Medicina basada en la evidencia y resultados del mundo real.

La transformación digital en el sector de la salud no es sino un cambio de mentalidad y cultura organizativa, y va más allá que la posibilidad de crear canales de comunicación entre pacientes y profesionales, los profesionales entre sí o los pacientes entre ellos, sino la posibilidad de extraer "inteligencia" de los datos a través de analítica avanzada gracias al *Big Data Sanitario*[59].

"La modernización tecnológica ha alcanzado también a las actividades de gestión y de prestación de servicios dentro del ámbito de la *administración sanitaria*, y a pesar de que pueden existir problemas que aún subsisten, se puede afirmar que en su mayoría los documentos en papel físico han sido sustituidos por el soporte electrónico y las comunicaciones telemáticas. Así por ejemplo, la información del paciente se está adaptando progresivamente a la movilidad nacional y europea donde su HCE incorpora información del mismo, sino que además se posibilita la accesibilidad telemática desde dispositivos móviles permite al paciente llevar a cabo tratamientos avanzados de dicha información médica, desde una perspectiva más amplia como las investigaciones observacionales o la gestión de los servicios. También la modernización ha permitido renovar el sistema de dispensación de medicamentos a través de la *receta electrónica*. Las tecnologías de la información y de la comunicación se caracterizan por la movilidad y la ubicuidad de los dispositivos así como por las posibilidades de interconexión que permiten las redes actuales, en especial a través de la telefonía móvil y de la conexión a Internet" (Valero, 2014, 633)[60].

En otro orden de cosas, antes de avanzar debemos hacer un alto para señalar las diversas fuentes de datos "heterogéneas". Concretemos dos posibles elementos antecesores a la e-Health: los HCE y la telemedicina.

2.2.1. Los Historiales Clínicos Electrónicos (HCE)

[59] Al inicio, los datos que se trataban tenían que ver con información no médica (gestión de pacientes, admisión, nóminas..etc.), pero posteriormente se fueron extendiendo a servicios clínicos: laboratorio, informes de diagnóstico, historial clínica electrónico, receta electrónica y telemedicina.

[60]Valero Torrijos, J. (2014) . Régimen Jurídico de la transparencia en el Sector Público: del Derecho de acceso a la reutilización de la información. En Cap. 19 *Acceso, reutilización y gestión avanzada de la información en el ámbito de la Administración sanitaria: implicaciones jurídicas desde la perspectiva y de la innovación tecnológica*. Editorial Aranzadi.

La definición legal de *historia clínica* según el art. 3 de la Ley 41/2002 de 14 de Noviembre de la autonomía de paciente y de derechos y obligaciones en materia de información y documentación clínica es "el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial".

Para Carnicero[61] (2003), las funciones de la historia clínica son:

- "*Asistencial.* La misión principal de la historia clínica es proteger toda la información patográfica con objeto de prestar la mejor atención posible.
- *Docente*.
- *Investigación*, tanto clínica como epidemiológica.
- *Gestión clínica* y planificación de recursos asistenciales
- *Jurídico legal,* pues es testimonio documental de la asistencia prestada.
- *Control de calidad* asistencial.

Según este autor[62], "la (nueva) historia clínica informatizada o electrónica (HCE), que supone incorporar las Tecnologías de la Información y de las Comunicaciones (TIC) en el núcleo de la actividad sanitaria, tiene como consecuencia que la historia deja de ser un registro de la información generada en la relación entre un

[61]SEIS, Sociedad Española de Informática de la Salud (18 de diciembre de 2003). De la historia clínica a la historia de salud electrónica. *Informes SEIS*. Coord. J. Carnicero. Recuperado en https://docplayer.es/3607660-Informes-seis-de-la-historia-clinica-a-la-historia-de-salud-electronica-pamplona-18-de-diciembre-de-2003.html Pág. 24-5

[62] Los HCE tendrán un papel muy importante en la prestación de servicios de salud de mayor calidad reduciendo costes aunque no siempre existirán ventajas en su implantación. En EEUU, a raíz de una investigación solicitada por la *California Health Care Foundation* (CHCF) con la firma *Booz Allen Hamilton* donde intervinieron expertos de la industria de salud de varias disciplinas, prestadores, pagadores y expertos en informática de salud determinaron algunos aspectos que contribuyeron a frenar la evolución del HCE como que: (i) Se enfocaba el HCE excesivamente en asegurar el pago de los servicios prestados (o *fee-for-service*); (ii) Los procesos en salud son complejos ; (iii) Se enfocaba escasamente en el intercambio de información (integración e interoperabilidad) ya que la mayoría de los HCE operaban en redes cerradas y no se conectaban con otros sistemas. No obstante, la ACA (ley de protección al paciente y al cuidado de salud accesible) se ha optado por nuevas inversiones de tecnologías de análisis de datos, en intercambio de dicha información y en tecnologías. Para más info: http://www.pardell.es/el-estandar-hl7.html

paciente y un profesional o un centro sanitario, para formar parte de un sistema integrado de información clínica". Toda información de salud de un ciudadano deberá ser integrada, de forma que contenga la información de todos los contactos y episodios del paciente e incluir, al menos información procedente de los siguientes sistemas:

- "Bases de datos de la *tarjeta sanitaria*.
- Historias clínicas *actuales*, cualquiera que sea el lugar en que se hayan generado.
- Sistemas clínicos *departamentales,* como los de los laboratorios y servicios de diagnóstico por imagen.
- Programas de *promoción* para la salud y de *prevención* de la enfermedad.
- Centros sanitarios *concertados* o de *otros servicios* de salud.
- *Contingencias* de salud laboral.
- Sistema de *receta electrónica*.
- Prestaciones sanitarias *complementarias*.
- Sistemas de ayuda a la toma de decisiones clínicas"

¿Y quiénes serán los usuarios o clientes de la HCE? Se pueden agrupar en los siguientes ámbitos: servicios sanitarios, servicios sociales, salud pública, gestores, servicios y administrativos y social (donde el paciente tiene un papel activo).

Pero para que se lleven a cabo los correspondientes intercambios de información es necesario que los personas estén debidamente identificadas (de forma inequívoca y unívoca). En nuestros país el DNI o el documento de afiliación a la Seguridad Social carecen de la precisión que exige el sistema de información clínica, por lo que en la década de los 90 se inició la identificación de los usuarios y se asignaros *las tarjetas sanitarias* y códigos de identificación personal por parte de los servicios de salud. En estas tarjetas sanitarias la información no está estandarizada (ni en la banda magnética ni en la base de datos). Según Carnicero, "su utilidad como instrumento de se ha puesto en evidencia con el desarrollo de los sistemas de información clínica sobre todo al relacionar sistemas distintos, como la historia de atención primaria con la de especializada o ambas, con los sistemas departamentales". En todo caso, según este autor, parece que lo más adecuado sería que "cada comunidad autónoma asigne un número de identificación y que sea de utilización exclusiva para el sistema sanitario, sin que pueda ser empleado por otras instancias". Acceder a la información clínica por medio de su identificación unívoca (y así localizar su información cumpliendo los requisitos de seguridad y confidencialidad) no debería dar problemas cuando está siendo

atendida dentro del ámbito en el que se le ha asignado el código (Madrid), pero sí los puede haber cuando acude a un centro en otra comunidad autónoma, como Andalucía. En estos casos, "se precisan necesariamente de estándares de intercambio de información y directorios que permitan la localización de la información existente"

Los datos pueden recogerse[63] con intervención de una persona o pueden ser capturados directamente de la fuente sin esa intervención (Carnicero):

- *Método personal:* es el más utilizado en los sistemas de salud y se produce cuando la información es generada o modificada por una persona. Puede ser directo, cuando la persona que la produce la introduce en el sistema e indirecto cuando se utiliza otra persona interpuesta. El registro de información con carácter personal puede seguir el modelo del *lenguaje natural o el modelo estructurado (por medio de guiones o plantillas, formularios, etc.)*. No obstante, según el autor, "cualquiera que sea el método utilizado, y sobre todo en el lenguaje natural, deben adoptarse criterios sobre el lenguaje y la terminología empleada".

- *Método no personal.* Se produce cuando la información se captura directamente desde *dispositivos y máquinas*, volcándose directamente en el sistema.

Las Administraciones Públicas o las empresas del sector privado coproveedores de salud tendrán en cuenta que los *historiales clínicos electrónicos* en el futuro deberán:

- Integrarse con *tecnologías y dispositivos* móviles que permita la recogida de datos no personal. Piénsese en el Apple watch y los informes que genera o la apps socialdiabetes.

[63] En este sentido, conviene tener en cuenta respecto a la *recogida de datos y presentación en el HCE* , los siguientes aspectos, según *Carnicero*: (i) No se puede presentar lo que no se ha registrado. (ii) La estructura con la que se dote a la información condicionará su presentación, almacenamiento y análisis. (iii) La estructura de los datos está condicionada por su naturaleza y por su origen. (iv) El dato debe ser introducido donde es generado y por quien lo genera, evitando pasos intermedios sin valor añadido, que además aumentan las posibilidades de error. (v) El dato debe ser introducido una sola vez. (vi) Debe quedar constancia de cualquier modificación o actualización e impedirse la modificación concurrente del dato. (vii) El origen del dato debe estar identificado. (viii) El dato debe estar identificado en el tiempo, indicando la fecha y hora en que se produce.

- Poseer *más capacidad de integrarse e interoperar* con otros sistemas y tecnologías con el fin de que aumente la participación del paciente y su comunicación con los prestadores de servicios de salud. Piénsese en la posibilidad de registrar los HCE en cadenas de bloques donde los participantes puedan intercambiarlo en el marco de un consorcio o asociación (hospitales, universidades, farmacéuticas, aseguradoras, etc.)

- Tener más *accesibilidad*, usabilidad y capacidad de *personalizar las herramientas*. Por ejemplo, en Estonia, los ciudadanos ya podrían acceder a su HCE.

- Ser capaces de adaptarse y desarrollarse conforme surjan nuevas *regulaciones o políticas públicas*. Piénsese en el escenario de cambio que se encuentran desarrolladores de software o informáticos médicos ante normativas como el RGPD.

- Interoperar de forma segura gracias a medidas de seguridad como anonimización, protocolos de control de acceso[64] de personal, software implementados para evitar posibles *vulneraciones en la privacidad*[65]. La mejora en el manejo de la información clínica implica en cierta parte un "*incremento del riesgo para la protección de la privacidad de los usuarios*, de manera que la efectiva adopción de las medidas de seguridad adquiere una transcendencia reduplicada".

Respecto a esta última consideración, detengámonos para comentar un par de *sentencias* que muestran la necesidad y repercusión de vulneraciones de protección de datos en los HCE:

[64] AEPD (octubre de 2010). *Informe de cumplimiento de la LOPD en Hospitales*. Recuperado en http://www.herbogeminis.com/IMG/pdf/aepd2.pdf. Según la AEPD, en el 88,4% de los centros el personal de gestión y control sanitario tiene limitado el acceso a las historias clínicas de los pacientes, y la mayoría de centros sanitarios (94,8%) han implantado medidas técnicas que impiden el acceso de terceros no autorizados o la difusión de datos de carácter personal de los ficheros del centro sanitario (limitación de la descarga de programas de intercambio de archivos, cortafuegos, etc.)

[65] Fernandez hierro. J.L. (2002). *Régimen jurídico general de la historia clínica*. En la obra coordinada *La Historia Clínica* por él mismo, pp. 172-6.Edit. Comares, Granada.

- Sentencia Tribunal Superior de Justicia de Navarra 2/2012, de 8 de febrero de 2012[66], confirmó una condena de 125.000 euros al Servicio Navarro de Salud por el acceso "ilegítimo" y masivo (2.800 veces se accedió al HCE), por parte del personal sanitario, al historial clínico de una paciente fallecida. Se evidenció que las medidas de seguridad y protocolo de trabajo en la Administración sanitaria no garantizaban la protección de datos.

A) Datos de identificación del enfermo y de la asistencia	
– Nombre y apellidos del enfermo. – Fecha de nacimiento. – Sexo. – Código de identificación personal contenido en la tarjeta sanitaria individual. – Domicilio habitual y teléfono. – Fecha de asistencia y de ingreso.*	– Indicación de la procedencia, en caso de derivación desde otro centro asistencial. – Servicio o unidad en que se presta la asistencia.* – Número de habitación y de cama, en caso de ingreso. – Médico responsable del enfermo.
B) Datos clínico-asistenciales	
– Antecedentes familiares y personales fisiológicos y patológicos. – Descripción de la enfermedad o del problema de salud actual y motivos sucesivos de consulta. – Procedimientos clínicos empleados y sus resultados, con los dictámenes correspondientes emitidos en caso de procedimientos o exámenes especializados y también las hojas de interconsulta. – Hojas de curso clínico, en caso de ingreso. – Hojas de tratamiento médico. – Hoja de consentimiento informado.* – Hoja de información facilitada al paciente en relación con el diagnóstico y el plan terapéutico prescrito.* – Informes de epicrisis o de alta, en su caso.	– Documento de alta voluntaria, en su caso. – Informe de necropsia, si existe. – En caso de intervención quirúrgica, debe incluirse la hoja operatoria y el informe de anestesia, y en caso de parto, los datos de registro. – El informe de urgencia. – La autorización de ingreso. – El informe de anatomía patológica. – En su caso, el documento de voluntades anticipadas, así como posible condición de donante de órganos. – La evolución y planificación de los cuidados de enfermería. – La aplicación terapéutica de enfermería. – El gráfico de constantes. – El informe clínico de alta.
C) Datos sociales	
– Informe social.*	

* Si procede.

Imagen 6. Tabla de contenido de un HCE en Navarra[67].

- La Sentencia de la Audiencia Nacional 437/2008, de 27 de febrero de 2008[68] sanciona infracción del deber de secreto, declarando la necesidad de *anonimizar* las historias clínicas cuando vayan a ser objeto de publicación. Se señaló que "los datos contenidos en las historias clínicas de los pacientes están protegidos por el deber de secreto exigido al responsable del fichero que contenga dichos datos de carácter personal. Era precisamente ese deber de secreto el que obligaba a anonimizar las historias clínicas que se facilitaron a la Administración Catalana para realizar el estudio estadístico que llevó a cabo, sin que la

[66]Vid. Sentencia Tribunal Superior de Justicia de Navarra de 8 de febrero de 2012. Recuperado en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=6283325&links=servicio%20navarro%20de%20salud&optimize=20120225&publicinterface=true

[67] Recuperado en http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1137-66272011000100008

[68]Vid. Sentencia de la Audiencia Nacional 437/2008, de 27 de febrero de 2008. Recuperado en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=181372&statsQueryId=104385084&calledfrom=searchresults&links=&optimize=20080403&publicinterface=true

obligación de colaboración con dicha Administración permitiera desatender las exigencias sobre protección de datos de carácter personal".

2.2.2. La Telemedicina

La OMS (1997), la consideró como "el suministro de servicios de atención sanitaria, en los que la distancia constituye un factor crítico, por profesionales que apelan a las tecnologías de la información y de la comunicación con objeto de intercambiar datos para hacer diagnósticos, preconizar tratamientos y prevenir enfermedades y heridas, así como para la formación permanente de los profesionales de atención a la salud" [69]. La telemedicina es la práctica de la atención médica a través de computadoras, redes de comunicación, tecnología médica y el personal de expertos del área de la salud que se apoyan en estas herramientas para poder prestar servicios a pacientes remotamente (Hailay y Roine, 2002)[70]. Entre estos servicios podemos encontrar: diagnóstico, consulta y tratamiento, educación sanitaria y transferencia de información médica a través de las comunicaciones audiovisuales y datos [71] (Stowe y Hardind, 2010)[72]. Según *Sánchez-Losada* (2017) se podrían señalar los siguientes conceptos en función del tipo de escenario[73]:

i. *"Teleasistencia:* interacción entre un médico y un paciente situado a distancia, normalmente aislado geográficamente y en situación de urgencia médica. Puede incluir o no Servicios de Telealarma. Así por ejemplo, la Fundación Recover conecta a médicos de hospitales africanos con facultativos voluntarios españoles.

---

[69] Por ejemplo, la Telemedicina en oncología mediante tecnologías inalámbricas, les permite ofrecer atención sanitaria con expertos, ayudando a la prevención, detección precoz, cuidados paliativos y rehabilitación en el tratamiento del cáncer remotamente en sitios de difícil acceso. En Bangladesh, donde la mayoría vive en zonas rurales que carecen de atención especializada, la necesidad de sistemas de telemedicina basados en Internet es mucho más grande, lo que permitiría a un gran número de médicos Salud Uninorte. Vid. Busra US, Dept. of Comput. Sci. & Eng. JUS, Dhaka, Bangladesh, Rahman MZ, editors. *Mobile phone based telemedicine service for rural Bangladesh: ECG.* Computer and Information Technology (ICCIT), 2013 16thInternational Conference on; 8-10 March 2014: IEEE.

[70] Hailay D, Roine R. (2002) Systematic review of evidence for the benefits of telemedicine. *J Telemed Telecare* ;8:1-77.

[71] Stowe S, Harding S. (2010) Telecare, telehealth and telemedicine. *European Geriatric Medicine* ;1:193-7.

[72] Comisión Europea (2018). *Market study on telemedicine. Final Report*. Recuperado de https://ec.europa.eu/health/sites/health/files/ehealth/docs/2018_provision_marketstudy_telemedicine_en.pdf

[73] Sanchez Losada, J.A. (2011). *Aspectos éticos y médico-legales en la Telemedicina: la consulta médica telefónica.* (Tesis doctoral, Universidad Complutense). Pp. 18-9. Recuperado de http://eprints.ucm.es/13892/1/T33350.pdf

ii. *Televigilancia:* seguimiento de enfermos crónicos o sujetos a algún tipo de intervención médica, desde su domicilio, mediante la recogida por vía telemática de informaciones médicas (tensión arterial, electrocardiograma, etc.). Esta forma de telemedicina se utiliza frecuentemente con pacientes que padecen enfermedades crónicas como diabetes o hipertensión.

iii. *Tele consulta entre médicos* (interconsulta): Se trata de la interacción entre dos médicos, uno encargado del paciente, y otro especialista o experto en un campo determinado que coopera telefónicamente u "online" con el médico responsable del paciente (teleradiología, telepatología, telecardiología, telelaboratorio).

iv. *Teleconsulta entre paciente y médico* (telefónica o web): El paciente busca directamente la opinión de un médico con el que no ha tenido una relación previa, y que no le ha realizado un examen clínico. Puede incluir Teleasistencia o no. Puede existir una cierta discusión acerca de la extensión de la responsabilidad del profesional que realiza un diagnóstico a través de esta vía[74].

v. *Telepresencia:* que supone la asistencia de un profesional sanitario remoto a un paciente, como en el caso de telediagnóstico mediante sistemas de videoconferencia en tiempo real. (No obstante, esto puede suponer algunos *inconvenientes*[75].Así por ejemplo, según *Kidscare*, compañía especializada en servicios médicos en escuelas infantiles, "la telepediatría podría evitar 3,6 millones de visitas al año en consultas de urgencias, suponiendo un ahorro superior a los 187 millones de euros año. Estas consultas se hacen en horario lectivo de lunes a viernes, por ello, la telepresencia sería el perfecto aliado para las 9.700 escuelas infantiles con 459.000 niños de 0 a 4 años registradas en España. Se utiliza material avanzado como cámaras de alta calidad, un pulsioxímetro y un fonendoscopio digital" [76]).

vi. *Telemonitorización:* que hace referencia a vigilancia remota de parámetros fisiológicos y biométricos de un paciente. En este sentido, *la* ***monitorización remota o telemonitorización*** **de personas con enfermedades crónicas** es una de las aplicaciones de la salud móvil que más desarrollo está sufriendo en los últimos años, ya que permite el seguimiento y control del paciente en el propio

[74]Vid. Sentencia núm. 106/2008 de 13 marzo. Audiencia Provincial de Murcia (Sección 1ª). AC 2008\978. Jurisdicción: Civil. Recurso de Apelación núm. 296/2007. (En la misma se señaló que el profesional (Ginecólogo) no se ajustó al "lex artis" al realizar un diagnóstico erróneo a distancia, por teléfono y sin haber practicado todas las pruebas diagnósticas previas).

[75] En 2007, se abrió un proceso disciplinario por el *General Medical Council* contra el *Dr. Julian Edel*, fundador de *e-Med*, un servicio de consulta médica a través de internet y teléfono que en ninguna ocasión realizó una conversación con los pacientes o con sus médicos sino únicamente por correo electrónico, sin realizar preguntas y examen físico. La parte contraria (GMC) encontraba en este, un sistema fácil para la obtención de fármacos -las recetas llegaban por correo ordinario- que deseara el médico sin necesidad de realizar examen físico o consulta en rigor. Recuperado de http://www.dailymail.co.uk/news/article-1211037/Internet-doctor-prescribed-drugs-suspended-struck-off.html

[76] SaludDigital (5 de mayo de 2018). Telepediatría en las escuelas para ahorrar visitas al médico. *SaludDigital Atención Sanitaria*. Recuperado de https://www.consalud.es/saludigital/109/telepediatria-en-las-escuelas-para-ahorrar-visitas-al-medico_49993_102.html

domicilio, anticipando la aparición de complicaciones antes de que el paciente acuda a los servicios de salud[77]. (Un ejemplo de la monitorización en el control y seguimiento remoto de pacientes con enfermedad crónica en España es el ***programa Valcronic de la Agencia Valenciana de Salud***[78]).

Imagen 7. Esquema de procesos en la comunicación con centrales de emergencia a través de la monitorización del programa Valcronic de Valencia. Fuente: SaludConectada

vii. *Telecirugía:* que hace uso de la tele robótica, la visión artificial y la realidad virtual".

2.3. Concepto eHealth y tipos.

La definición más referenciada es la de *Eysenbach*[79] publicada en la editorial JMIR en 2001:

"e-Health abarca más allá de un mero desarrollo tecnológico; en concreto se parte de un sentido más amplio, como si se tratara de un estado de ánimo, una manera de pensar, una actitud y un

[77] Esto se lleva a cabo mediante una serie de sensores y dispositivos que recogen datos clínicos del paciente, los cuales son enviados a una central, en los que un profesional sanitario, los procesa y actúa en función del estado del paciente. Estos servicios posibilitan por tanto ofrecer un apoyo a la atención de determinados grupos de pacientes que tienen necesidades especiales, como por ejemplo: *procesos crónicos, cuidados paliativos, medicina de urgencias*, etc. Los sistemas suelen ser interactivos e incluyen *sistemas de alarma* que ponen en marcha procedimientos de comunicación con centrales de asistencia en caso de urgencia, desde los cuales distintos profesionales pueden solicitar información, consultar el historial clínico del paciente y ofrecer consejos y orientaciones de forma remota.

[78] SaludDigital. Ejemplos para entender la Salud Digital (III*): Organizaciones sanitarias*. 3. *Innovación en Organizaciones sanitarias.* Blog. Recuperado en https://saludconectada.com/salud-digital-innovacion-organizaciones/. (Incluye dos modalidades de intervención en España: por un lado, controlar y hacer seguimiento de la patología crónica mediante sistemas de telemonitorización y por otro, mejorar los hábitos de vida saludable y fomentar el autocuidado, a través de contenidos de educación para la salud. Con él se pretende aumentar el grado de control de las patologías crónicas mediante la comunicación con el paciente y un seguimiento presencial y a distancia. Esto se traduce en una mayor calidad de atención, un incremento de la eficiencia y eficacia, y la prevención del ingreso del paciente, manteniéndole el mayor tiempo posible en su domicilio).

[79] Eysenbach G. (2001). What is e-health? J Med Internet Res. Apr-Jun;3(2):E20. PubMed PMID: 11720962; PubMed Central PMCID: PMC1761894. Recuperado en http://www.jmir.org/2001/2/e20/

compromiso para el pensamiento en red, global, para mejorar la atención de salud a nivel local, regional, y en todo el mundo mediante el uso de tecnologías de información y comunicación."

El primer plan de acción a favor de un Espacio Europeo de la Salud Electrónica[80] (2004) estableció hace más una década que la *e-Health* tenía una importancia capital, ya que podía mejorar el acceso a la asistencia sanitaria y multiplicar la calidad y la eficacia de los servicios ofrecidos. Este plan entendía por salud electrónica:

> " la aplicación de las tecnologías de la información y las comunicaciones en la totalidad de las funciones que afectan al sector de la salud. Entre las herramientas o soluciones asociadas a la salud electrónica figuran productos, sistemas y servicios que van más allá de las meras aplicaciones basadas en Internet. Incluyen herramientas para uso tanto de las autoridades sanitarias como de los profesionales, así como sistemas de salud personalizados para pacientes y ciudadanos. Sirvan de ejemplo las redes de información sanitaria, las historias clínicas informatizadas, los servicios de telemedicina, los sistemas de comunicación personales vestibles y transportables, los portales de salud y muchas otras herramientas basadas en las tecnologías de la información y las comunicaciones cuyo objetivo es facilitar la prevención, el diagnóstico, el tratamiento, el seguimiento de la salud y la gestión del estilo de vida."

Así, el segundo plan de acción (2012-2020)[81] [82] define y llega a afinar -en la misma línea – el concepto de la salud electrónica como:

> "el uso de las TIC en los productos, servicios y procesos sanitarios, combinado con cambios organizativos y nuevas capacidades en los sistemas de atención sanitaria, a fin de mejorar la

[80] Comisión de las Comunidades Europeas (30 abril de 2004). *La salud electrónica – hacia una mejor asistencia sanitaria para los ciudadanos europeos: Plan de acción a favor de un Espacio Europeo de la Salud Electrónica.* (SEC(2004)539). Recuperado en http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52004DC0356&from=EN

[81] Comisión Europea (6 de diciembre de 2012). *Plan de acción sobre la salud electrónica 2012-2020: arLa salud electrónica – hacia una mejor asistencia sanitaria para los ciudadanos europeos: Plan de acción a favor de un Espacio Europeo de la Salud Electrónica.* Ver en http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52012DC0736&from=EN

[82] Comisión Europea (2018) . *Consultation: Transformation Health and Care in the Digital Single Market.* Recuperado en: https://ec.europa.eu/health/sites/health/files/ehealth/docs/2018_consultation_dsm_en.pdf. (Resulta de interés que se señale que"La mayoría de los encuestados confirmaron que en la actualidad no tienen acceso a la salud digital y que servicios de atención médica. De los que no lo hacen, a dos de cada tres encuestados les gustaría que el oportunidad de acceder a estos servicios digitales y el 83,6% reconoce que la innovación digital, la retroalimentación de los ciudadanos puede mejorar los servicios de atención de salud. Con el fin de abordar el bajo nivel de adopción de soluciones digitales de salud en la atención de la salud, el los encuestados se mostraron favorables a una inversión sostenida de la UE en investigación e innovación, a la transferencia de tecnología y a la creación de empleo. conocimientos y prácticas entre los EEMM y las regiones, y enfoques comunes para mecanismos de retroalimentación sobre la calidad del tratamiento").

salud de los ciudadanos, la eficacia y la productividad de la prestación de dicha atención, así como el valor social y económico de la salud**.** La salud electrónica abarca la interacción entre los pacientes y los proveedores de servicios sanitarios, la transmisión de datos de unas instituciones a otras o la comunicación entre pares entre los pacientes y/o los profesionales de la salud"

Como podemos ver en el segundo plan resalta el término "interacción" entre pacientes y proveedores sanitarios y "comunicación" entre pacientes y profesionales de la salud. Desde mi humilde punto de vista, prefiero desglosar el concepto en:

i. La interacción e "intercambio de información" entre pacientes y proveedores de servicios (como son hospitales o centros de salud).
ii. La transmisión de información entre instituciones o empresas
iii. La comunicación e "intercambio de información" entre:
    a. Pacientes y profesionales de la salud
    b. Pacientes y pacientes
    c. Profesionales de la salud

Ahora bien, de manera más específica y por cuanto nos interesa, parece adecuado el siguiente esquema de eHealth:

2.3.1. La m-Health.

La Comisión Europea[83] (2018) señaló que: "las herramientas digitales, como las aplicaciones de salud móviles o los dispositivos personales para controlar la sangre o el azúcar, permitirán a las personas cuidar su salud, mejorar la prevención de enfermedades y permitir la retroalimentación e interacción entre los usuarios y los proveedores de atención médica"**.**

Según la OMS[84] (2011) se considera como un subcomponente de *eHealth* en términos de "práctica médica y de salud pública respaldada por dispositivos móviles, como teléfonos móviles, dispositivos de monitoreo de pacientes, PDA y otros dispositivos inalámbricos".

[83] Comisión Europea (25 de abril de 2018) *Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society*. Recuperado en https://ec.europa.eu/digital-single-market/en/news/communication-enabling-digital-transformation-health-and-care-digital-single-market-empowering.

[84] La Organización Mundial de la Salud cree que casi el 90% de la población mundial podría beneficiarse de las oportunidades que brindan las tecnologías móviles. Según el último informe del ISM Health el 30% de aplicaciones están orientadas únicamente a profesionales y pacientes mientras que el 70· restante están orientadas al público general (monitorización de hábitos saludables, por ejemplo).

Para el científico Robert Istepanian (2004) *m-Health* engloba ampliamente el uso de las telecomunicaciones móviles y las tecnologías multimedia, ya que se integran en un entorno cada vez y los sistemas de prestación de servicios de salud inalámbrica[85]. Y de una manera similar la Fundación para los Institutos Nacionales de la Salud (FINH), en la cumbre m-Health de 2010, lo definió como "la prestación de los servicios de salud a través de dispositivos de comunicación móvil."

Los factores que propician la digitalización y la llegada de la tecnología a la industria del cuidado de la salud, se extienden al sector mHealth por lo que simplemente los enumeraremos: (i) *empoderamiento del paciente; (ii) modificación de hábitos* (actividad física, la dieta o tabaco); (iii) c*ambios de relaciones y procesos* donde profesionales de la salud utilizan tablets o Smartphone para analizar síntomas como el estado del ánimo, dolor, presión arterial, glucosa; (iv) *monitorización* donde los dispositivos móviles pueden hacer electrocardiogramas, medir la glucosa o la capacidad de oxígeno. El control remoto sobre todo ayuda a los pacientes en la gestión de la cronicidad[86]; (v) a*lmacenamiento inteligente de datos* provenientes de dispositivos[87],

[85]World Health Organization (2018). *Towards the Development of an mHealth Strategy: A Literature Review* pp 14. Recuperado en http://www.who.int/goe/mobile_health/mHealthReview_Aug09.pdf

[86]No obstante, existen un sistema de monitorización de salud para ancianos no invasivo que por medio de la señal wifi y de forma no invasiva la mejora la observación de las personas mayores . Ver más info en : https://www.consalud.es/saludigital/116/un-sistema-monitoriza-la-salud-de-los-ancianos-en-sus-domicilios_51954_102.html

[87] Jiménez, I (28 de abril de 2018). Cumpliendo con la GDPR. *Abogacía Española Consejo General. Blogs*. Recuperado en https://www.abogacia.es/2018/04/26/cumpliendo-con-la-gdpr/

Sin adelantarnos al capitulo de compliance y seguridad y análisis de riesgos, resulta de gran interés enumerar algunos riesgos de privacidad que acarrean los dispositivos móviles como señala *Iñigo Jiménez* en el CGAE (2018); "(i) *Facilidad de identificación.* Recientemente hubo un estudio en el que se llegó a identificar de forma precisa determinados dispositivos simplemente por la batería de estos, pues la capacidad de almacenamiento y los patrones de su carga/descarga hacen que cada batería sea única y por tanto sirve como elemento de identificación único; (ii) *Recolección constante de múltiples datos personales:* Gracias a los sensores que tienen los dispositivos móviles, tales como GPS, acelerómetro, giroscopio, micrófono, cámara, WIFI, estos están permanentemente generando datos personales, como ubicación, temperatura, redes a las que se conectan. Además, múltiples aplicaciones recolectan datos muy sensibles como pueden ser datos de salud, religión, sexo, afinidades políticas, aficiones, etc., pues, a la hora de identificarnos, permiten la identificación mediante nuestros perfiles en las redes sociales, con lo que los datos que compartamos en dichas redes (por ejemplo nombre, edad, contactos, etc.) podrán ser recolectados y usados por estas aplicaciones.
Con el auge de los asistentes personales, los dispositivos están con *el micrófono activado* a la espera de alguna instrucción, para el procesamiento de estas órdenes frecuentemente los sonidos grabados por los dispositivos son enviados para su interpretación a las *diferentes plataformas móviles*.
Y aunque no seamos conscientes de ellos, muchas aplicaciones usan librerías de terceros para poder tener informes estadísticos de uso de la aplicación; (iii) *Facilidad de acceso físico; (iv) Datos en la nube; (v) Dispositivo personal en la empresa:* Si el dispositivo se conecta a las redes WIFI de la empresa, nos tendremos que asegurar que ese dispositivo tiene las medidas de seguridad mínimas para evitar propagar cualquier tipo de *malware* y evitar filtraciones de documentación sensible y que además ese dispositivo está en la lista blanca de dispositivos que la organización permite conectarse. Además deberemos asegurarnos de que el dispositivo tiene activado el *cifrado*, y *métodos seguros de autenticación* (mediante

redes sociales, aparatos médicos y trabajarlos de forma que permita la predicción, prevención y personalización de enfermedades. El *Health Intelligence* ayudará a almacenar, procesar y generar información para la toma de decisiones médicas

Según la ICB[88], hay tres categorías de mHealth; aplicaciones relacionadas con el tratamiento, aplicaciones relacionadas con predicción y prevención, y aplicaciones relacionadas con el estilo de vida. La UE para dar luz a esta cuestión ha creado un directorio[89] de apps de salud con el fin de servir de apoyo a los pacientes para que encuentren apps útiles y fiables.

A continuación, señalamos algunos ejemplos de aplicaciones app:

Nombre	Características
"Instant Heart Rate"	Utiliza la cámara de un teléfono inteligente para detectar el color del dedo de un usuario y de esta manera detectar el pulso cardíaco[90].
"Fedediabetes"	Creada por la FEDE (Federación de Diabéticos Españoles) cuenta con un diario donde se puede incluir información del paciente sobre la medicación, valores de la glucemia, peso, tensión y citas con el profesor sanitario.
"Social diabetes"	Permite el registro de la dieta del paciente, la cantidad de insulina, de carbohidratos, base de datos de alimentos, un diario digital para registrar todos los datos personales e incluso posibilidad de contar con tele asistencia.
"One drop"	Al crear la cuenta se debe ingresar un nombre y la dirección de correo electrónico, aunque el paciente puede añadir voluntariamente el número de teléfono, el sexo, la altura y el peso, el tipo de diabetes, año de diagnóstico, rango de glucosa, la marca de la insulina y el medidor de la glucosa. Los usuarios-pacientes pueden cargar fotografía y etiquetan momentos con notas. Además, es posible que el usuario de el permiso a terceros (Apple HealthKit) para utilizar información. En la política de privacidad, se señala que One Drop puede anonimizar y agregar datos recogidos y usarlos para *cualquier propósito*.
"CatchMyPain"	Permite al usuario registrar lo que le duele, cuándo le duele, etc., para compartir esa

huella, patrón o contraseña o la combinación de éstos) y estableceremos una política de actuación en los casos de pérdida o robo de los dichos dispositivos. También es muy importante proporcionar una *guía a los empleados* en cuanto al uso seguro de los dispositivos tanto dentro como fuera de la organización *(no conectarse a redes WIFI públicas, no usar servicios de mensajería instantánea que no tengan cifrado punto a punto, etc.".*

[88] Comité Internacional de Bioética (15 de septiembre de 2017). *Informe del IBC sobre big data y salud.* Recuperado de http://unesdoc.unesco.org/images/0024/002487/248724e.pdf

[89] Patient View (2012). *European Directory of Health Apps 2012-2013. A review by patient groups and empowered consumers.* Recuperado en http://www.patient-view.com/uploads/6/5/7/9/6579846/pv_appdirectory_final_web_300812.pdf

[90] Recuperado de http://www.azumio.com/apps/heart-rate/

	información con el médico

Tabla 3. Ejemplos de aplicaciones mHealth

Respecto a lo que nos incumbe en este trabajo, hemos de decir, que uno de los desafíos clave del uso de mHealth cómo asegurar enfoques viables para la privacidad y la seguridad, en especial, en los países de ingresos bajos y medios (PIMB) (León y Schneider , 2012,19) [91].

2.3.2. La w-Health

Están en armonía con el cuerpo humano bien en forma de complementos, de dispositivo implantable o prenda de ropa. Tienen funciones que no solo sirven para la salud sino para mejorar la calidad de vida ya que ofrecen control continuo y en tiempo real de recopilación de datos relacionados con el organismo humano. Esto cambiará por completo la gestión de la información, ya que hará que los historiales clínicos serán más completos y complejos, a la vez que se creen perfiles personalizados con algoritmos para su interpretación. Enfermedades como la epilepsia, diabetes, esclerosis múltiple y la depresión encontrarán en estos dispositivos unas herramientas únicas para mejorar la calidad y esperanza de vida. Según el I Congreso Nacional de eSalud de 3 de Noviembre de 2016, por ejemplo, en el Hospital de la Paz anunciaron que cuentan con 3.000 dispositivos conectados cuyos pacientes mandan informe diariamente.

Algunos de los ejemplos de estos dispositivos con sensores pueden ser los mostrados en los últimos *Mobile Word Congress*:

Nombre	Carecterísticas
"Inodoros conectados"	detectan el cambio en la orina que puede derivar a problemas de salud
"Colchones conectado"	detectan la inmovilidad para evitar úlceras en personas inválidas
"Suelos conectados"	detectores de caídas

[91]Leon, N & Schneider H. (2012) *MHealth4CBS in South Africa: a review of the role of mobile phone technology for monitoring and evaluation of community based health services, South African Medical research services and the University of the Western Cape.* Recuperadode http://www.hst.org.za/publications/NonHST%20Publications/MHealth4CBS-A%20Review.pdf (A mi modo de ver, se trata de un problema "silenciado" donde en más de alguna ocasión se han salpicado noticias de escándalos públicos de empresas estadounidenses farmacéuticas que utilizaban de forma ilegítima datos personales de salud en países africanos).

"Vehículos conectados"	detectan comportamientos anómalos o problemas de salud del propio conductor y que emiten respuestas de emergencia en ciudades inteligentes
"Zapatos conectados"	con *gps* para personas con alzeheimer

Tabla 4. Ejemplos de dispositivos IoT

Es necesario, llegados a este punto, advertir que un *chip subcutáneo* no es un wareable ya que no se puede desprender en cualquier momento. Se rumorea que dentro de unos años posiblemente la implantación de chip[92] en humanos con fines de asistencia médica será una realidad, lo que se desconoce es si será voluntario u obligatorio. A los expertos legales que preocupa bastante sus implicaciones legales desde la perspectiva de la bioética clínica y de la bioética normativa[93]. Por la mayor o menor incidencia que pueden tener en la intimidad y privacidad de las personas, hemos de atender a la clasificación realizada por el Grupo Europeo de Ética de las Ciencias y las Nuevas Tecnologías de la Comisión Europea que distingue tres tipos de chip; (i) uno de solo lectura similar al que hoy día se les inserta sólo a los animales, (ii) otro de lectura/escritura y (iii) un tercer chip con función de localización y posibilidad de tratamiento de datos por parte de terceros, como el fabricante del soporte y que entroncaría las funciones del chip de lectura/escritura. *Las autoridades europeas alertan de los peligros que pueden acarrear al poder otorgar datos ajenos al tratamiento a terceros acerca de la salud de los individuos, aparte de los derivados para el uso de la tecnología de la domótica susceptibles de vulnerabilidades de seguridad informática.*

2.3.3. La e-Health

Es el uso de un conjunto específico de herramientas Web –blogs, *podscat, tagging,* búsqueda web, wikis, foros- por parte de los actores de la atención de la salud, incluyendo médicos, pacientes y científicos utilizando los principios de código abierto y la generación de contenidos por los usuarios, sumando al poder de las redes, con el fin

[92]En EEUU, un ciudadano lleva implantado un chip NFC bajo la mano con el cual pretende abrir la puerta de su casa, la del coche y la del garaje . (Vid en http://computerhoy.com/noticias/hardware/hombre-implanta-chip-nfc-su-propia-mano-20035).

[93] Suecia es pionera en la utilización de chips subcutáneos para acceder a datos personales sin prescripción médica a través de las tarjetas NFC *(Near Field Communication)* donde más de 3.000 personas de nacionalidad sueca se han implantado en el 2018 los chips subcutáneos para abrir puertas, registrarse o pagar peajes. (Para más info: https://www.clarin.com/sociedad/3000-suecos-implantaron-chip-electronico-datos-piel_0_rJkfU2rCf.html)

de personalizar la atención de la salud, colaborar y promover la educación para la salud[94].

Así por ejemplo, *Auffermann et al.* (2015) afirman que los servicios de redes sociales en Internet han cambiado la forma en que nos comunicamos como sociedad y ofrecemos oportunidades para mejorar la forma en que se practica actualmente la radiología[95]. Para *Lober y Flowers* (2011) el cambio acelerado de la tecnología en salud tienen sus raíces en las tendencias; en su trabajo revisan las actividades en la capacitación de los consumidores y la tecnología, y encontraron que las tendencias sociales son visibles en la integración de las tecnologías de la información y las comunicaciones en el área de la salud, tanto en la búsqueda y el intercambio de información en Internet, en el uso de los medios sociales para crear nuevos tipos de interacciones con la familia, proveedores y compañeros, y en el e-paciente, que integra estas nuevas funciones y nuevas tecnologías[96].

3. LA INDUSTRIA FARMACEUTICA DIGITAL

Por ejemplo, imaginemos un día de invierno. Nos levantamos y tenemos fiebre y un espantoso dolor de garganta. Abrimos una aplicación móvil en nuestro iphone y accedemos a nuestro registro de salud electrónico y respondemos una serie de preguntas que nos lanza el chatbot. Según los síntomas y la evidencia visual, la aplicación determina que es probable que tengamos en la garganta "estreptococos" (bacterias) que ha derivado en una faringitis. Emite una orden para una prueba de diagnóstico y nos envía a la farmacia local para comprar un "hisopo" y el tratamiento correspondiente.

[94] ONTSI (2015). Estudio sobre opiniones y expectativas de los ciudadanos sobre el uso y la aplicación de las TI en el ámbito sanitario. Recuperado de http://www.ontsi.red.es/ontsi/sites/ontsi/files/los_ciudadanos_ante_la_e-sanidad.pdf. (Casi 4 de cada 10 individuos comparten la información sanitaria que registran con sus dispositivos y aplicaciones con su médico (37,9%), especialmente los mayores de 65 años para el seguimiento de determinadas variables de salud (el 49,4% lo harían). Tan sólo en el 4% de los casos, el dispositivo o aplicación envía los datos directamente al profesional. Por su parte, el 16,3% lleva el dispositivo directamente al centro de salud para que los profesionales "descarguen" o extraigan los datos desde el dispositivo. Según esta encuesta, una de las limitaciones para los pacientes es el uso de los dispositivos y las app de salud son la protección de datos y la privacidad.)

[95] Auffermann WF, Chetlen AL, Colucci AT, DeQuesada Ii IM, Grajo JR, Heller MT et al. (2015), Online Social Networking for Radiology. *Academic Radiology* ;22(1):3-13.

[96] Lober WB, Flowers JL. (2011), Consumer Empowerment in Health Care Amid the Internet and Social Media. *Seminars in Oncology Nursing* ;27(3):169-82.

Es un ejemplo de Inteligencia Artificial y la industria del cuidado de salud previsto para el 2030 (Horihuela, 2018)[97] donde el paradigma farmacéutico está cambiando[98].

3.1. Cambio de paradigma: De Industria tradicional a la tecnológica.

3.1.1 Antecedentes.

Para poder hablar del cambio de paradigma sería interesante hacer antes un paso breve por la historia de la farmacia hasta la era de la moderna Industria Farmacéutica. En Babilonia, cerca del 2600 A.C., los médicos que practicaban el *arte del Apotecario* (del lat. *Apothecaius)* eran el sacerdote, el farmacéutico y el médico, todo en uno y venían utilizando *tabletas de arcilla* donde registraban los síntomas de la enfermedad, para componer una invocación a los dioses. En Egipto, el expediente más importante era el *"papiro Ebers"* con una colección de 800 prescripciones donde se mencionaban 700 drogas. Con la llegada de la Edad Media, los restos de conocimiento occidental de medicina y farmacia fueron preservados en los monasterios desde S.V al S, XII, en los cuales los monjes reunían hierbas del campo para curar a los enfermos y heridos. Pero no son sino con los árabes quienes consiguen separar el arte de la medicina del arte médico en *Bagdad*, cuando se crean las primeras farmacias de propiedad privada en el S.VIII. Con la llegada de los musulmanes a África y Europa, llevaron con ellos un nuevo modelo de farmacia que pronto se fue asimilando. Antes del siglo XX, la formulación y preparación de medicamentos se hacía por un solo farmacéutico o con el maestro farmacéutico. A partir del siglo XX, la elaboración de los medicamentos corre a cargo de la moderna *industria farmacéutica*, aunque siguen siendo farmacéuticos los que coordinan e investigan la formulación y preparación de medicamentos en las grandes empresas farmacéuticas. Según Wikipedia, la *Industria Farmacéutica*[99] convencional del S.XXI "se dedica a la fabricación, preparación y comercialización

[97] Horihuela, J. (23 de febrero 2018) Health care in 2030: AI And the Shifting Role Of Your Pharmacist. *Forbes.* Recuperado de https://www.forbes.com/sites/forbestechcouncil/2018/02/23/health-care-in-2030-ai-and-the-shifting-role-of-your-pharmacist/#104f13d032c5

[98] En el futuro, según algunas estimaciones, los proveedores de salud interactuarán estrechamente asumiendo el farmacéutico local funciones propias de asistencia sanitaria propias del médico en el caso de problemas no graves (aconsejando sobre diabetes o hacer trabajo de laboratorio para diagnostico). En EEUU van en la línea de cumplirlo, por ejemplo, la cadena farmacéutica CVS se ha fusionado con la aseguradora estadounidense de salud Aetna.

[99]Recuperado de https://es.wikipedia.org/wiki/Industria_farmac%C3%A9utica

de productos químicos medicinales para el tratamiento y también la prevención de las enfermedades". Ahora bien , conviene citar los dos tipos de organizaciones de esta industria:

a. Las que fabrican productos químicos farmacéuticos a *granel* (producción *primaria*).

b. Las que preparan para su uso médico mediante métodos conocidos colectivamente como producción *secundaria*. Por ejemplo, fármacos dosificados, como pastillas, cápsulas o sobres para administración oral, disoluciones para inyección, óvulos y supositorios. Existe una gran variedad de leyes y reglamentos con respecto a las investigaciones, patentes, pruebas y comercialización de estos fármacos[100].

Según algunos los críticos, los altos precios no estarían en relación directa con la inversión en la investigación sino, más bien, con las ganancias producidas por la comercialización de los medicamentos[101][102].

3.1.2. La llegada de la nueva Industria Farmacéutica Tecnológica[103].

En la era de la Sociedad de la Información, el paciente cuenta con los datos integrados en el móvil con diferentes apps y los proveedores de salud pueden realizar el seguimiento y control a través de sus datos de forma segura y creando informes que podrán ser integrados en el HCE del hospital o en los registros médicos de las aseguradoras o mutuas. Las características de la nueva "Industria Farmacéutica

[100] La mayoría de los países conceden patentes para los medicamentos o fármacos recientemente desarrollados o modificados, por periodos de unos 15 años a partir de la fecha de autorización. Las compañías asignan una marca registrada a sus innovaciones, que pasan a ser de su propiedad exclusiva. Además, los nuevos medicamentos reciben un nombre genérico oficial de propiedad pública. Una vez que expira la patente, cualquier empresa que cumpla las normas del organismo regulador puede fabricar y vender productos con el nombre genérico.

[101] Champagne, D., Hung, A., Leclerc, O. (dic. 2015). Cómo las farmacias pueden ganar en un mundo digital. *Blog McKinsey & Company Productos farmaceuticos y productos médicos.* Recuperado de https://www.mckinsey.com/industries/pharmaceuticals-and-medical-products/our-insights/how-pharma-can-win-in-a-digital-world

[102] Autores argumentan "los pocos medicamentos que son verdaderamente innovadores generalmente se han basado en investigaciones respaldadas por los contribuyentes realizadas en centros médicos académicos sin fines de lucro o en los Institutos Nacionales de Salud". La industria farmacéutica estima que cada nuevo medicamento les cuesta $ 800 millones para desarrollar y llevar al mercado, pero autores comoAngell y Relman estiman que el coste es en realidad cercano a los $ 100 millones).

[103] Según *McKinsey*, "las proyecciones sugieren que los mercados de la industria farmacéutica en India y China tendrá un crecimiento anual del 17% durante los próximos cinco años, mientras que los mercados de dispositivos médicos crecen al 11% y 22% en cada país respectivamente , superando ampliamente el crecimiento general regional de las balanzas comerciales. Durante los últimos 10 años, los flujos comerciales de dispositivos médicos y farmacéuticos han crecido al menos el doble de rápido de las balanzas comerciales en manufactura en promedio". Recuperado de https://www.mckinsey.com/industries/pharmaceuticals-and-medical-products/our-insights

Tecnológica" -si se puede llamar así- según la consultora *McKinsey*[104] son las siguientes:

i. *Las personas controlarán sus propios tratamientos de salud.* El *Dr. Bertalan Meskó* establece que: "la atención médica será impulsada mucho más por los consumidores que por los médicos". Por otro lado, *Dan Goldsmith*, el director de estrategia de *Veeva Systems*, lleva la idea más allá: "en los próximos tres a cinco años en lugar de que los pacientes solo estén informados y sean más inquisitivos, diseñarán activamente los enfoques terapéuticos y de tratamiento para ellos mismos con sus médicos". Cada vez más, las empresas tecnológicas estudian a fondo como se relacionan los pacientes y sus médicos. Por ejemplo, observan el comportamiento a través de comunidades virtuales, participan en foros de comunidades de investigación y utilizan métodos cuantitativos para analizar tendencias. Ahora bien, tal y como establece el *Dr. Todd Johnson*, CEO de Noble.MD: "Las aplicaciones que estén diseñadas para resolver las *necesidades comerciales* de las compañías farmacéuticas nunca deberían existir" (ver capítulo ética).

ii. *El entorno clínico cambiará. L*os médicos necesitarán nuevas habilidades, herramientas y capacitación, por ejemplo, deberán ser capaces de integrar datos de miles de dispositivos portátiles y otras tecnologías de "autocomprensión cuantificada". Piénsese en la píldora de hipertensión *Diovan*, con el *chip Proteus* integrado.

Imagen 8. Diovan pildora con microchip. Fuente: Protesus[105]

El chip registra el momento en que el paciente toma una píldora y transmite esta información desde el interior del cuerpo a un parche que el paciente usa. Esta información se puede enviar a un Smartphone, a un PC y a cloud donde pacientes y proveedores de salud puedan acceder a ella.

iii. *Las compañías farmacéuticas pueden perder el control exclusivo sobre sus historiales de valor.* Éstas no podrán controlar totalmente los datos de sus productos, *salvo que interactúen con terceros* (otros sectores o comunidades). Deberán ser transparentes de cara a los ensayos clínicos para que puedan confiar los pacientes, y en consecuencia, los legisladores. La tendencia y desafío del futuro, será la transformación

[104] Idem.
[105] Recuperado de http://www.proteus.com/discover/

de las compañías farmacéuticas en meras "*compañías de fármacos"* en "*compañías de soluciones"*. A medida que las empresas sanitarias y las tecnológicas lleguen al dominio farmacéutico, las compañías farmacéuticas necesitarán renovar sus propuestas de valor de manera significativa.

3.2. Transformación digital y fuente de datos

Aunque la digitalización en el sector farmacéutico se ha resistido al cambio, grupos farmacéuticos y laboratorios importantes generan a diario gran cantidad de información. Volviendo nuevamente a la cuestión de estudio que nos centra referente a los datos y a la privacidad, en ese mismo informe de McKinsey se menciona también que:

> "Para desarrollar las combinaciones más prometedoras de manera eficiente, estas compañías farmacéuticas necesitan *acceder y compartir los primeros datos* y mejorar su infraestructura digital para administrar ensayos complejos y presentaciones en forma conjunta. Múltiples "terceros" están agregando datos de salud y poniendo a disposición de proveedores y pagadores los datos y las estadísticas".

Por su parte, también se plantean que uno de los desafíos que enfrentan los fabricantes de fármacos es establecer *relaciones más estrechas con los pacientes* (Van Den Heuvel, 2017)[106]. Dos cambios sísmicos están afectando a la industria: la necesidad de demostrar el valor de las terapias; y el paso del tratamiento a la prevención, el diagnóstico y la cura, todo lo cual atrae a una gran cantidad de nuevos competidores. Como resultado a estos desafíos cada vez más empresas farmacéuticas, tecnológicas y de dispositivos médicos se están asociando[107]. Nos referimos a colaboraciones como:

[106]Van Den Heuvel, R. (6 de febrero de 2017). Pharma outlook 2030: From evolution to revolution. *KMPG*. Recuperado de: https://home.kpmg.com/xx/en/home/insights/2017/02/pharma-outlook-2030-from-evolution-to-revolution.html?cid=linkd_soc_xx-acx_adv-pharma2030&utm_medium=soc&utm_source=linkd&utm_content=xx-acx&utm_campaign=adv-pharma2030&sf54814790=1

[107] Google, Microsoft y Apple registran más de 300 patentes de salud desde 2013. Solo **Alphabet** (matriz de **Google), Microsoft y Apple** han solicitado 313 patentes de atención médica en Estados Unidos desde 2013, según el informe *Life Sciences 4.0* de la consultora EY. Alphabet lidera esas invenciones con 186

Nombre de Farmacéutica y Tecnológica	Actividad
Sanofi - Alphabet	Crean la joint venture Onduo, como una clínica virtual contra la diabetes
Microsoft -Novartis	Desarrollar dispositivos que se utilicen frente a las enfermedades crónicas
Berkshire Hathaway y JP Morgan Chase Amazon	Abaratar la costosa atención médica en Estados Unidos.
Johnson & Johnson -HP	Tecnología de impresión 3D aplicada a la salud
Pfizer- IBM Watson	Investigación en inmunoncología.
GSK - Alibaba	Ayuda médica online sobre la vacuna frente al papiloma humano.

Tabla 5. Ejemplos de colaboraciones entre organizaciones tecnológicas y farmacéuticas.

Actualmente, según EY, la mayor parte de las alianzas entre laboratorios y tecnológicas están en el campo de diabetes, seguido de respiratorio, oncología, neurología o cardiovascular.

3.2.1.Aplicaciones móviles (apps).

Desde la Asociación de profesionales de la farmacia se publicó la "*FarmaAPPedia*"[108], un libro con formato digital donde se recopilan las aplicaciones para la prescripción o la gestión de la farmacia. Algunas son:

Nombre	Actividad
RecuerdaMed.	Permite recordar la medicación mediante un sistema de alarmas, útil para personas con enfermedades crónicas que tienen varios cuidadores.
MediSafe.	Sirve para organizar los fármacos en función del color y la forma. Además, tiene la opción de incluir distintos usuarios a quienes se les mandan notificaciones para controlar la correcta toma de los tratamientos.

solicitudes, seguida de Microsoft con 73 y Apple con 54. Llama la atención el poder de las tecnológicas frente a las empresas farmacéuticas. Si las empresas de ciencias de la salud descartan entrar en estas plataformas, corren el riesgo de ser marginadas por la nueva tecnología y los competidores digitales", se recoge en el informe. Al fin y al cabo, el futuro estará marcado por la "economía de datos", un mercado único donde los gigantes de internet llevan ventaja.

[108] Vid. Cachafeiro Jardón, M.J. (2018). La FarmAPPedia. *Catálogo de APPs de uso y preescripción en la Farmacia.* Recuperado de https://www.dropbox.com/s/wzs44nnkh30gz4g/La%20FarmAPPedia.pdf?dl=0

MyPill	Se utiliza para el control de anticonceptivos mediante un sistema de alarmas que requiere un registro previo. Existen dos versiones: gratis y de pago
Medicamento Accesible Plus	Es una app dirigida a personas mayores con problemas visuales que tengan dificultad a la hora de leer los prospectos de los medicamentos.
INR Control	Está diseñada por la Federación Española de Asociaciones de Pacientes con el objetivo de ayudar a mantener un mejor control del índice de coagulación del usuario. También dispone de una guía completa de información sobre los problemas de coagulación.
AlerHTA	Sirve para registrar la tensión y las pulsaciones del usuario así como cuenta con consejos sobre hábitos de vida saludables.
Social Diabetes	Permite introducir los valores de los controles de glucemia, registrar la administración de insulina o medicamentos antidiabéticos orales y consultar recomendaciones dietéticas
MySugar	Esta aplicación también es para las personas con diabetes para mantener un mejor control de la patología.
RespirApp	Es de la Asociación Española Contra el Cáncer para los usuarios que deseen dejar de fumar
Kwit.	Al igual que la anterior es para dejar el tabaco pero a través de un juego
Polen Control	Sirve para medir los niveles de polen y registrar los síntomas en las personas con alergias. Está avalada por la Sociedad Española de Alergología e Inmunología Clínica.
Mi embarazo al día	Permite monitorizar los cambios durante la gestación e incluye una guía con recomendaciones
LactApp	Las usuarias pueden resolver sus dudas sobre la lactancia y registrar las tomas.
iPediatric	Incluye una pediátrica para padres.
¿Qué puedo comer?	Identifica los alérgenos utilizando una base de datos compuesta por más de 100.000 productos españoles.
Nefrodiet	Ayuda a controlar la alimentación de pacientes con diálisis, hemodiálisis o diálisis peritoneal y cuenta con el apoyo de la Sociedad Española de Nefrología y la Sociedad Española de Enfermería Nefrológica.
FotoSkin.	Sirve para hacer un seguimiento de los lunares y las manchas en la piel.

SolFarma	Editada por el Consejo General de Colegios Oficiales de Farmacéuticos incluye información sobre fotoprotección.
Vacunas 3.0	Se trata de un manual sobre los calendarios y las necesidades de vacunación durante los viajes al extranjero.
Viajar Sano	Como la anterior, esta app indica las vacunas necesarias para viajar.
YoTeCuido Alzheimer.	Está dirigida a los cuidadores con información y ejercicios para que también se cuiden ellos mismos.

Tabla 6. Ejemplos de apps de farmacéuticas.

3.2.2. Big data y la Industria Farmacéutica

Por otro lado, se encuentra también esta tecnología en el ámbito de la Ind. Farmacéutica, que genera ciertos beneficios como son hacer los diagnósticos más eficaces, las mejoras en la planificación e interpretación de resultados, la creación de patrones de enfermedades, la mejor predicción de la seguridad y la eficiencia de un medicamento, la medición con precisión de la eficacia de los visitadores y el ahorro de costes. Algunos ejemplos de utilización de la tecnología en la Industria Farmacéutica son los siguientes:

Nombre Farmacéutica	**Actividad**
AstraZeneca	Desarrollo de fármacos controlados por Analytics con Big Data
Bayer	Aceleración de ensayos clínicos con Big Data
GSK	Aumento de las tasas de éxito en el descubrimiento de fármacos con Big Data
Johnson & Johnson	Intelligent Pharmaceutical Comercialización con Big Data
Medtronic	Facilitación de la atención predictiva con Big Data
Merck & Co	Optimización de la fabricación de vacunas con Big Data

Merck KGaA	Descubrimiento de medicamentos más rápido con Big Data
Novartis	digitalización de la asistencia sanitaria con Big Datos
Pfizer	Desarrollo de terapias eficaces y específicas con Big Data
Roche	Personalización de la atención médica con Big Data
Sanofi	Atención proactiva a la diabetes con Big Data Proveedores de atención médica, aseguradores y pagadores
Aetna	predicción y mejora de la salud con Big Data
Bangkok Hospital Group	Transformar la experiencia del paciente con Big Data
Gold Coast Health	Reducir los tiempos de espera en el hospital con Big Data
IU Health (Indiana University Health)	Prevención de infecciones adquiridas en hospitales con Big Data
MSQC (Michigan Surgical Quality Collaborative)	Mejora de calidad quirúrgica con Big Data
NCCS (Centro Nacional del Cáncer de Singapur)	Avanzando en el tratamiento del cáncer con Big Data
NHS Escocia	Mejora de los resultados con Big Data
Seattle Children's Hospital	Permitir un diagnóstico más rápido y preciso con BigData
UnitedHealth Group	Mejora de la atención y el valor del paciente con Big Data
VHA (Veterans Health Administration)	Agilización de la prestación de servicios de salud con Big Data
Amino	Transparencia de la atención médica con Big Data CosmosID: avance microbiano Genómica con Big Data
Express Scripts	Mejora de la adherencia a los medicamentos con Big Data
Faros Healthcare	Mejora de la toma de decisiones clínicas con Big Data Genomics England: desarrollo del primer servicio de medicina genómica del mundo con Big Data
Ginger. io	Mejorando el Bienestar Mental con Big Data
Illumina	Habilitando la Medicina de Precisión con Big Data

INDS (Instituto Nacional de Datos de Salud, Francia	Manejo de la Salud de la Población con Big Data
MolecularMatch	Avance de la Utilidad Clínica de la Genómica con Big Data
Proteus Digital Health	Medicina Digital pionera con Big Data
Royal Philips	Mejora de los flujos de trabajo en UCI (unidades de cuidados intensivos) con Big Data
Sickweather	Pronóstico de enfermedad y mapeo con Big Data

Tabla 7. Ejemplos de utilización de big data en la Industria Farmacéutica.

Es por todo ello, que ***Farmaindustria***[109] **está trabajando en el desarrollo de un *nuevo código de conducta* de protección de datos personales** en el ámbito de la **investigación clínica y de la farmacovigilancia.** En él se pretende garantizar el adecuado equilibrio entre la protección de datos personales obtenidos en el entorno clínico y el fomento de la investigación biomédica, en un momento en el que el proceso de digitalización permite generar una **gran cantidad de información** que tiene a su vez un enorme potencial de cara a favorecer la I+D de nuevos medicamentos.

3.2.3. Inteligencia Artificial y la Industria Farmacéutica

La inteligencia artificial, además del Big Data, facilitará la labor de los médicos en la búsqueda de un diagnóstico, algo que ayudará a reducir la repetición innecesaria de pruebas y visitas a especialistas así como errores diagnósticos.

[109]RedacciónMédica (15 de noviembre de 2017). Nuevo código de la industria para proteger datos personales en "Big Data". *Redacción Médica.* Ver en: https://www.redaccionmedica.com/secciones/industria/nuevo-codigo-de-la-industria-para-proteger-datos-personales-en-big-data--8696 (El nuevo código vendrá a actualizar el modelo de corregulación en materia de protección de datos actualmente vigente en el ámbito de la industria farmacéutica, haciendo que las responsabilidades y derechos sean compartidos por todos los agentes implicados con la finalidad de dar respuesta a los nuevos retos que las diferentes fuentes de *big data* -información genómica, ensayos clínicos, historia clínica electrónica, etcétera- están planteando en este ámbito, como por ejemplo la seudonimización -tratamiento de datos personales que impide que se atribuyan a una persona sin recurrir información adicional-, la gestión de hallazgos incidentales o el fomento del uso de repositorios de datos genómicos. Los objetivos del este código entre otros son uniformizar criterios en la recogida de datos, la obtención del consentimiento y el proceso para pseudonimizar los datos).

Así por ejemplo, la herramienta *SirFinder* es un software que utiliza la inteligencia artificial en la biofarmaceutica en Sylentis, del grupo PharmaMar y el grupo AIA. Su objetivo es potenciar el desarrollo de fármacos que interactúan con este ARN. Esta herramienta permitirá generar miles de compuestos específicos para determinadas enfermedades" [110].

Por otro lado, un caso real de resultado de la asociación de la tecnología de Inteligencia artificial y la industria farmacéutica es *Mendelian*[111]. Esta nueva plataforma y motor de búsqueda permite que un especialista o laboratorio de genética con un caso sin diagnosticar pueda acceder a la plataforma, sin necesidad de registrarse previamente, introducir las características fenotípicas del paciente, y por medio de los algoritmo, ofrecerá una lista de genes potencialmente responsables y mutaciones específicas. Una vez incluidos los datos fenotípicos sobre la enfermedad del paciente, el algoritmo recorre toda la información disponible sobre estas patologías y sus causas, procedentes de *bases de datos públicos, terminólogos, casos reales, publicaciones científicas,* etc., hasta proporcionar un resultado ordenado por probabilidad[112].

Los datos se codifican de manera inconsistente o no están codificados, lo que no permite que los datos se fusionen. En general, los datos de los sitemas de salud y los ensayos clínicos se recopilan para fines "extremadamente" específicos (Perkslis, 2017[113]). Y es que al margen de la gestión de datos que se puede hacer en los HCE (con objetivos de facturación, más bien) o en los ensayos clínicos (gracias a los protocolos), está algo que importa mucho a la Industria Farma y es la "gestión del conocimiento" donde los datos se extraen, se vuelven a formatear y se convierten como en un almacé de datos. Más del 90% del esfuerzo en proyectos de aprendizaje automático en el mundo real terminará centrado en la limpieza y gestión de datos (Imran Haque). Ahora bien, muchos investigadores, para solucionar el problema de la calidad de datos han decidido desarrollar sus propios conjuntos de datos (la mayoría datos preclínicos), es el

[110] S.Nadal, MV (26 de diciembr de 2018). Algoritmos para acelerar la investigación de fármacos. Retina *El País Economía.* Recuperado de https://retina.elpais.com/retina/2018/12/21/innovacion/1545388739_968425.html?Id_externo_rsoc=TW_CM_RT_bc_phm

[111] Vid www.mendelian.co

[112] La plataforma tiene indexadas 10.713 enfermedades raras y genéticas. Se persigue realizar un estudio socio-sociosanitario para analizar los costes directos e indirectos de 500 enfermedades raras y modelizar el coste oportunidad del retraso del diagnóstico, entre otros.

[113] Vid. https://venturevalkyrie.com/new-tech-tonics-podcast-eric-perakslis/

caso de *Recursion Pharmaceuticals*. En definitiva, los sistemas de IA serán buenos si lo son sus datos. Los datos si no son bien utilizados sólo son basura.

Respecto al buen uso del software (en dispositivos médicos) e IA en la industria farmaceutica, es de señalar la implicación de la FDA estadounidense, creando documentos a modo de guidelines abordando cuestiones legales-eticas que afectan[114].

3.3.4. Blockchain y la Industria Farmacéutica

El intercambio de datos y la preocupación por la protección de datos de los individuos en la participación en ensayos clínicos son enormes desafíos médicos para la investigación clínica contemporánea. Pero Blockchain podría ser clave para enfrentar estos desafíos y debe llamar la atención de toda la comunidad de investigación clínica. Los fabricantes de medicamentos que llevan a cabo ensayos clínicos podrían *compartir* datos clínicos y muestras médicas de forma más *segura*[115] *, sencilla e interoperable.* Según un estudio, el 60% de las compañías farmacéuticas actualmente utilizan o experimentan con *blockchain*[116] .

El problema es que los métodos actuales de recolección de pruebas de ensayos clínicos son caros[117], lentos e ineficientes. Las organizaciones de investigación por contrato suelen tardar más de un año en compilar las pruebas de ensayos manualmente a partir de silos de la industria, a menudo completando esto con más estudios. Y los pacientes no reciben *compensación* cuando se "venden" sus datos agregados y la base legitimadora del tratamiento de datos correspondiente (consentimiento explícito) no siempre estaría cubierto. Pero además de esa falta de legitimación, hay problemas de calidad de los datos agregados o de la gestión dado a la escasa interoperabilidad[118] y posibilidad de portarlos. Esto dificulta encontrar y reclutar individuos con los criterios

[114] Vid. https://www.healthcareittoday.com/2019/06/20/fear-and-confusion-over-the-software-and-artificial-intelligence-revolution-reaches-the-fda/ y https://www.regulations.gov/docket?D=FDA-2019-N-1185

[115] En un modelo descentralizado en el que todos los hospitales cuentan con una base de datos *distribuida, transparente y segura* mediante criptografía y son los pacientes quienes tienen el control de la información los problemas de ciberseguridad podrían evitarse. Además, la gestión de la identidad supone asimismo un eje fundamental para combatir un problema actual en hospitales, el Ransomware.

[116] Benchoufi, M, Ravaud, P. (19 de julio de 2017). Blockchain technology for improving clinical research quality. *BMC Trialsjournal*. Recuperado de https://trialsjournal.biomedcentral.com/articles/10.1186/s13063-017-2035-z

[117] Palomas D. (20 de abril de 2018). ¿Cuál es el coste de desarrollar nuevos medicamentos?. *Dciencia.* Recuperado de http://www.dciencia.es/cual-es-el-coste-de-desarrollar-nuevos-medicamentos/

[118] Vid. https://amp.redaccionmedica.com/secciones/sanidad-hoy/la-receta-electronica-espanola-se-conectara-con-europa-a-partir-de-2021-1375

más idóneos para la realización de pruebas bajo rigurosos controles. En este punto, la tecnología *Blockchain* permitiría a las personas que desearan participar en los ensayos *agregar* los *datos asociados* con su salud y hacerlos *visibles* para todos los reclutadores asociados con las empresas farmacéuticas[119]. Ya hay iniciativas en marcha como:

Nombre	Actividad
Robomed Network	Es un red médica virtual que ofrece *smart contracts* para los pacientes y proveedores donde se comparte información médica.
MedRec[120]	Emplea *software de Ethereum* para construir una *blockchain privada* asociando a diferentes proveedores de asistencia médica permitiendo que compartan información.
Health Co	Trata de establecer una relación directa entre pacientes e investigadores.
The BlockRx Project[121]	La plataforma es una solución integral para integrar completamente a los investigadores, *BioPharma,* fabricantes de dispositivos médicos y proveedores de atención médica para mejorar los resultados del paciente.
Zenome[122]	Permiten monetizar los datos genómicos[123],.

Tabla 8. Ejemplos de utilización de blockchain en la Industria Farmacéutica.

Pero incluso, se puede llegar más lejos. La empresa *Bowhead Health*[124]cuenta con un dispositivo que controla los *datos biométricos* de un cliente para dispensar

[119] De este modo, los reclutadores podrían seleccionar a la persona en base a la información de sus registros y a este último le llegará una notificación, la cual, si es aceptada, revelará al reclutador los datos de identificación del participante para que este sea contactado.
[120] Recuperado de https://medrec.media.mit.edu/ (El usuario sería propietario directo de los datos y podría decidir de forma personal si ceder o *comercializar* esos datos para aquellas iniciativas que considerase oportunas, y contaría con un incentivo para a portar esa información de tan elevado valor para empresas e investigadores. Esta información será la del genoma humano personal**,** nutrición o estado físico personal, el genoma de ascendientes, el microbioma).
[121] Ver en: https://www.blockrx.com/ (Fecha consulta 19 mayo 2018)
[122]Vid. en: https://zenome.io/ (Fecha consulta 19 mayo 2018)
[123] El valor de mercado de los datos genéticos alcanzó los $ 5.9 mil millones en 2010 una cifra que se prevé que crecerá significativamente en los próximos años. Sin embargo, en la actualidad, un pequeño número de corporaciones genómicas , empresas farmacéuticas e instituciones científicas y médicas controlan toda la información disponible Vid. https://futurism.com/23andme-is-raising-200-million-to-make-drugs-from-your-dna/ (Fecha consulta 19 mayo 2018)

suplementos y medicamentos personalizados veganos. Los clientes y los poseedores de token de Bowhead serían compensados por el "*arrendamiento de datos médicos"* y los pacientes tendrían el control total de sus datos por medio de *smart contracts con Hyperledger*. En su whitepaper se puede leer; "los usuarios tienen control total sobre si, cuándo, dónde y cómo comparten sus datos". El funcionamiento de esa compartición de datos se explica de la siguiente manera (parte inferior izquierda):

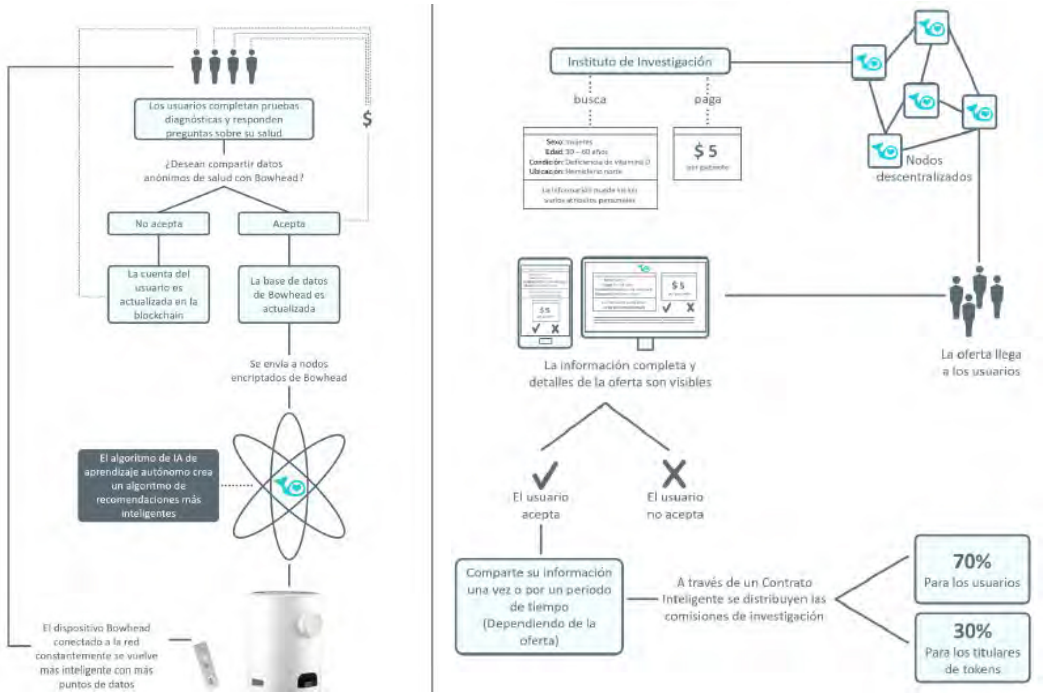


Imagen 9. Funcionamiento (ciclo vida datos) de Bowhead Health. Fuente: Bowhead

En la parte posterior derecha, se muestra también, cómo los pacientes podrían ser *recompensados* a través de un aumento de los tokens por compartir sus datos de salud. Señalan que "el paciente se convierte en el único que puede controlar el quién, qué, cuándo y cómo de esos datos". Si una institución de investigación o compañía farmacéutica quisiera "comprar datos", los participantes y los titulares de tokens pueden beneficiarse enormemente.

En definitiva, la tecnología *Blockchain* posibilita un nuevo paradigma y ecosistema en las relaciones de los sujetos jurídicos o participantes (ver gráfico inferior a modo de ejemplo). Piénsese que los *farmacéuticos,* como proveedores de salud, podrán averiguar si un medicamento está resolviendo o no el problema de un paciente,

[124]Vid. https://www.bowheadhealth.com/ Ver whitepaper en https://drive.google.com/drive/u/0/folders/0B2CimLH8gflNeUMwUWNXa3VrX2M

si éstos sufren algún efectos secundarios, si un paciente está al día con sus vacunas (y en caso negativo, administrar las necesarias), o si el paciente sigue el tratamiento (es decir, cómo es la adherencia a los medicamentos recetados). Y algo importante para resolver los grandes problemas de interoperabilidad en los sistemas de salud; puede averiguar si el paciente ha recibido preescripción excesiva de ciertos analgésicos, por ejemplo, y en ese caso intervenir. Es decir, se plantea un escenario lleno de posibilidades para la ayuda del paciente (*).

Imagen 10. Ejemplo de ecosistema de stakeholders con tecnología blockchain.

Por su parte, "en la Industria farmacogenómica, los científicos están aprendiendo que los medicamentos hechos a la medida o las dosis personalizadas de los medicamentos existentes, diseñados para igualar las predisposiciones genéticas de grupos de individuos con rasgos genéticos similares, pueden ayudar a salvar vidas y tratar enfermedades de manera más eficiente" (Koepsell, 2019)[125]

4. LA INDUSTRIA ASEGURADORA DE LA SALUD DIGITAL

[125] Vid. https://www.himss.org/news/genomic-data-and-blockchain-new-paradigm-precision-medicine-and-science y http://sitn.hms.harvard.edu/flash/2018/understanding-ownership-privacy-genetic-data/

Los orígenes se remontan a las Hermandades y Cofradías de *carácter gremial*, mediante las cuales los trabajadores se unieron al objeto de encontrar de forma colectiva una indemnización o asistencia en caso de enfermedad. Este carácter gremial tenía el inconveniente que no llegaba a la totalidad de la población. A finales del siglo XIX y a principios del s. XX, la clase médica generaliza las conocidas "*igualas",* donde se pasa de contar con un médico a tener un grupo especialistas ampliándose la oferta sanitaria. La aprobación de la *Ley de Seguros de Diciembre de 1954*, obligó a las Entidades que operaban en este ramo a ir adaptándose a la misma y a convertirse en *Sociedades Anónimas.* En los años 70-80 las sociedades aumentan los aseguradores que quieren una especie de medicina privada (pero más asequible). En esta fecha nacen empresas aseguradoras como Adeslas o Sanitas.

Vistos los antecedentes de la industria, conviene tratar algunas características. En primer lugar, es necesario conocer que la naturaleza del riesgo del seguro de salud puede ser , bien , un suceso futuro como es una enfermedad, o bien, eventos ciertos y reales como una visita a un médico. Todo posible asegurado será candidato y deberá cumplir una serie de requisitos y políticas (condiciones de asegurabilidad) que fija la Compañía como el cuestionario médico y/o las pruebas médicas, y las normas de suscripción. Se sabe que con la edad las personas son más propensas a padecer ciertas enfermedades, sobre todo si no toman medidas preventivas y no se mantienen costumbres saludables. Por ello, la selección de riesgos tiene en cuenta el historial clínico de la persona y el estado de salud que tiene en el momento de solicitar el seguro. Son los llamados *factores médicos*[126].

4.1.Cambio de paradigma y transformación digital .

[126] Los factores médicos que influyen son: (i) *Hábitos* de salud (IMC, toxicología, ejercicio físico..). El índice de masa corporal (IMC) es una medida estadística del peso de una persona con respecto a su altura. Se calcula dividiendo el peso corporal entre la altura elevada al cuadrado. Los Profesionales de la salud lo usan para calcular si una persona está por debajo del peso normal, tiene peso normal, sufre de sobrepeso o si es obesa. La Organización Mundial de la Salud definió el IMC como el estándar para evaluar riesgos asociados al sobrepeso en adultos. El Tabaquismo y el Alcoholismo forman parte de los malos hábitos de la persona que pueden deteriorar su salud y hacerla propensa a tener ciertos padecimientos. La actividad física puede dar una vida más longeva y saludable. El ejercicio es una ayuda para la prevención de las enfermedades del corazón, y muchos otros problemas físicos, además de reducir la ansiedad y tensión. También es una buena manera de cambiar el rumbo del apetito y quemar calorías ; (ii) *Historia clínica y estado de salud personal.* A través del historial clínico de la persona se pueden determinar las preexistencias y el estado de salud que tiene en el momento; (iii) *Historia clínica familiar.* El historial de salud de la familia puede resultar interesante para identificar afecciones actuales y potenciales (o patologías de tipo hereditario). Suele ser considerado un factor importante ya que puede reflejar predisposición a tener algún padecimiento.

Según *Deloitte*, "la industria de los seguros tiene una particularidad probablemente única: vende el mismo producto desde sus orígenes hace siglos. Esto podría llevar a concluir que es un sector que *no avanza ni se transforma,* sin embargo, es todo lo contrario, hay muchas cosas que están cambiando en la industria aseguradora a nivel mundial y a nivel de la región"[127]. Gracias a los nuevos recursos digitales, las compañías tienen por primera vez a su alcance medios atractivos y beneficiosos para acercarse a sus agentes o corredores generando así posibilidades de acceso, personalización y contacto, a costes razonables. A ello se une el cambio en la mentalidad, hábitos y comportamientos de los clientes[128] [129].

Un ejemplo de empresa proveedora tecnológica que trabaja con tecnologías emergentes IoT, IA y Blockchain y tiene clientes que son aseguradoras es *Bodyo*. El papel que tomarán es de responsables del tratamiento, en tanto que decidan los medios y las finalidades del tratamiento de datos. Y los encargados serán dichas empresas proveedoras tencnológicas (Bodyo, Microsoft, etc.…) junto con los subcontratistas proveedores tecnológicos (desarrolladores SC, etc.). Por ejemplo, con la tecnología blockchain y los smart contract tienen un sistema de recompensa para los pacientes que muestran un buen comportamiento de salud.

Fuente Bodyo

[127] Oliva, F., Flores, M. La transformación de las compañías de seguros en la era digital. *Deloitte Análisis.* Recuperado de https://www2.deloitte.com/uy/es/pages/strategy-operations/articles/La-transformacion-de-las-companias-de-seguros-en-la-era-digital.html

[128] Vid. https://nae.global/posicionamiento-digital-de-las-aseguradoras-generales-en-espana-i/. El gráfico que señala NAE es bastante significativo para comprender la situación actual en nuestro país.

[129] Según esta consultora hay cinco cambios clave de la era digital : (i) *"Social: un nuevo paradigma de la compra de seguros"*. Es social porque las personas valoran cada vez más la opinión de los demás. Los nuevos clientes jóvenes que entran en el mercado están totalmente integrados en la era digital. Aparecen "*marketplaces*" de seguros en el mundo con gran éxito, como por ejemplo *Insurify.com* o el más cercano *Comparaencasa.com*. donde se puede hacer lo mismo que en *Amazon* pero comprando un seguro. (ii) *Móvil: un canal ideal para el servicio post venta, además de generar mejoras en la oferta de servicios. (iii) Pricing: el retorno de las pólizas a la medida.* Vinculado con el punto anterior, surge otro fenómeno que se denomina el "Internet de las Cosas" (*IoT – Internet of Things*). Esto implica usar el rastro digital que las personas van dejando para obtener un mejor precio por sus pólizas de seguros. Una aplicación de este nuevo concepto es el "pago por el uso": si se aceptan las condiciones, por ejemplo, *compartir la información del GPS del celular con la compañía de seguros*, ella podrá evaluar la forma en que cada día se usa el automóvil, las rutas que se eligen, los horarios en los que se maneja, velocidad, etc. (iv) *Analytics: la información como base de la transformación.* Por ejemplo: una persona joven que acaba de tener su primer hijo es seguramente candidato ideal para comprar un seguro de vida, como así una persona con varios hijos que estén iniciando la edad escolar es un target para un seguro de matriculación, y un turista es target para un seguro de viaje. (v) *Insurtech: ¿enemigos o aliados?* Muchas tecnologías tienen el potencial de lograr impactos relevantes, un ejemplo obvio es la tecnología blockchain.

La digitalización ha llegado tan fuerte a esta industria que aseguradoras tan grandes como la americana "*John Hancock"* dejará de suscribir el seguro de vida tradicional y solo trabajará con "*pólizas interactivas"*. La novedad más importante es la obligatoriedad de que el cliente se someta a un seguimiento de la condición física y los datos de salud a través de dispositivos wearables, como pulseras de actividad y relojes inteligentes o Smartphone. Con esta situación, los asegurados tendrán descuentos por alcanzar objetivos de ejercicio físico quedándose registrados sus datos de salud en los dispositivos *FIT bit o Apple Watch* y pueden obtener tarjetas regalo, descuentos en su póliza y otras ventajas registrando sus entrenamientos diarios[130]. Este nuevo escenario ha creado revuelo y debate en el sector de la privacidad planteando cuestiones como si las aseguradoras están legitimadas para usar datos y así, "*seleccionar a los clientes más rentables"*, mientras aumentan los cobros a aquellos que no participan de los programas de actividad física. Las respuestas las podremos encontrar en la RGPD como veremos a continuación.

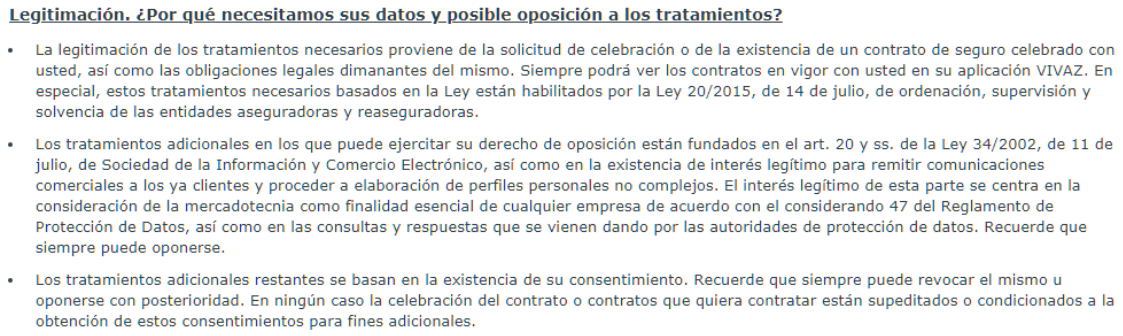
Llegados a este punto, y para alcanzar una dimensión más práctica, y aunque en este capítulo no hemos abordado aún el régimen jurídico aplicable, me gustaría tomarme la licencia de adelantar de forma breve algunos aspectos significativos y comentarios de la política de privacidad ("y la información por capas") de "aseguradoras digitalizadas de salud" tomando de referencia alguna compañía española "*Vivaz*[131]*,* de la Compañía Línea Directa";

Respecto a la legitimación (ver capítulo 8, aptdo. 6.2). La aseguradora justifica la legitimación jurídica de los tratamientos de datos en el art. 6.1.b.RGPD ("el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales") y también, en 6.1.c RGPD ("el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento") cuando se refiere a la Ley 20/2015 y la necesidad de dichos tratamientos. Para el resto de tratamientos como la remisión de comunicaciones comerciales y tratamiento automatizado tienen otras legitimaciones jurídicas (ej. interés

[130]Reuters (20 de septiembre de 2018). Sin pulsera de actividad no hay seguro de vida, la nueva estrategia aseguradora en EEUU. *El Economista.* Recuperado de https://www.eleconomista.es/empresas-finanzas/noticias/9400218/09/18/Sin-pulsera-de-actividad-no-hay-seguro-de-vida-la-nueva-estrategia-aseguradora-en-EEUU.html ("En teoría, todos ganan, ya que los titulares de las pólizas se sienten incentivados a adoptar hábitos saludables y las compañías de seguro cobran más primas y pagan menos en reclamaciones si los clientes viven más tiempo")

[131]Vid. https://www.vivaz.com/politica-de-privacidad-ampliada.html

legítimo). El interés legítimo, en este caso último, se encaja en la "mercadotecnia como finalidad esencial de cualquier empresa (considerando 47 RGPD). El lector y usuario también entiende que puede oponerse en cualquier momento. Para el resto de tratamientos, determina que su legitimación es el consentimiento, informándole que no se utilizarán para fines adicionales[132].

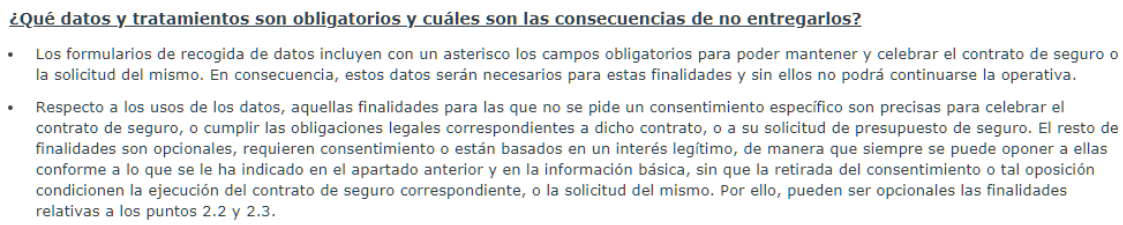


Legitimación. ¿Por qué necesitamos sus datos y posible oposición a los tratamientos?

- La legitimación de los tratamientos necesarios proviene de la solicitud de celebración o de la existencia de un contrato de seguro celebrado con usted, así como las obligaciones legales dimanantes del mismo. Siempre podrá ver los contratos en vigor con usted en su aplicación VIVAZ. En especial, estos tratamientos necesarios basados en la Ley están habilitados por la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.
- Los tratamientos adicionales en los que puede ejercitar su derecho de oposición están fundados en el art. 20 y ss. de la Ley 34/2002, de 11 de julio, de Sociedad de la Información y Comercio Electrónico, así como en la existencia de interés legítimo para remitir comunicaciones comerciales a los ya clientes y proceder a elaboración de perfiles personales no complejos. El interés legítimo de esta parte se centra en la consideración de la mercadotecnia como finalidad esencial de cualquier empresa de acuerdo con el considerando 47 del Reglamento de Protección de Datos, así como en las consultas y respuestas que se vienen dando por las autoridades de protección de datos. Recuerde que siempre puede oponerse.
- Los tratamientos adicionales restantes se basan en la existencia de su consentimiento. Recuerde que siempre puede revocar el mismo u oponerse con posterioridad. En ningún caso la celebración del contrato o contratos que quiera contratar están supeditados o condicionados a la obtención de estos consentimientos para fines adicionales.

Imagen 11. Clausula legitimación de la aseguradora Vivaz. Fuente: Vivaz. Línea Directa.

Respecto a la obligatoriedad de los mismos y sus consecuencias[133] *esto es lo que señala:*



¿Qué datos y tratamientos son obligatorios y cuáles son las consecuencias de no entregarlos?

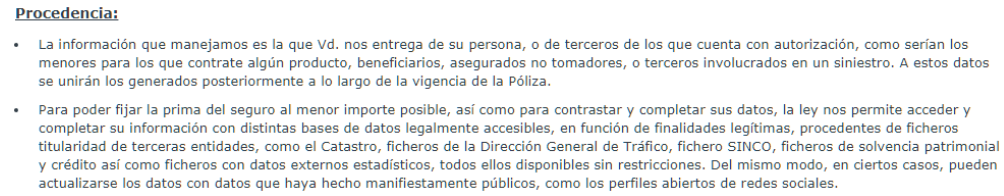
- Los formularios de recogida de datos incluyen con un asterisco los campos obligatorios para poder mantener y celebrar el contrato de seguro o la solicitud del mismo. En consecuencia, estos datos serán necesarios para estas finalidades y sin ellos no podrá continuarse la operativa.
- Respecto a los usos de los datos, aquellas finalidades para las que no se pide un consentimiento específico son precisas para celebrar el contrato de seguro, o cumplir las obligaciones legales correspondientes a dicho contrato, o a su solicitud de presupuesto de seguro. El resto de finalidades son opcionales, requieren consentimiento o están basados en un interés legítimo, de manera que siempre se puede oponer a ellas conforme a lo que se le ha indicado en el apartado anterior y en la información básica, sin que la retirada del consentimiento o tal oposición condicionen la ejecución del contrato de seguro correspondiente, o la solicitud del mismo. Por ello, pueden ser opcionales las finalidades relativas a los puntos 2.2 y 2.3.

Imagen 12. Clausula datos y tratamientos obligatorios de la aseguradora Vivaz. Fuente: Vivaz. Línea Directa.

Respecto a la procedencia. La aseguradora informa al potencial asegurado las fuentes de información; ficheros de terceras entidades, Catastro, ficheros de la Dirección Feneral de Tráfico, fichero SINCO, ficheros de solvencia patrimonial y crédito, ficheros con datos externos estadísticos. Y algo muy importante: " del mismo modo, en ciertos casos, pueden actualizarse los datos con datos que haya hecho manifiestamente públicos, como los perfiles abiertos de Redes Sociales". A mi modo

[133] El Art. 13.2.e señala que "si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos".

de ver, esta cuestión es particularmente delicada y requeriría que fuera destacada a la vista del individuo, indicando qué RRSS y el alcance de la información.

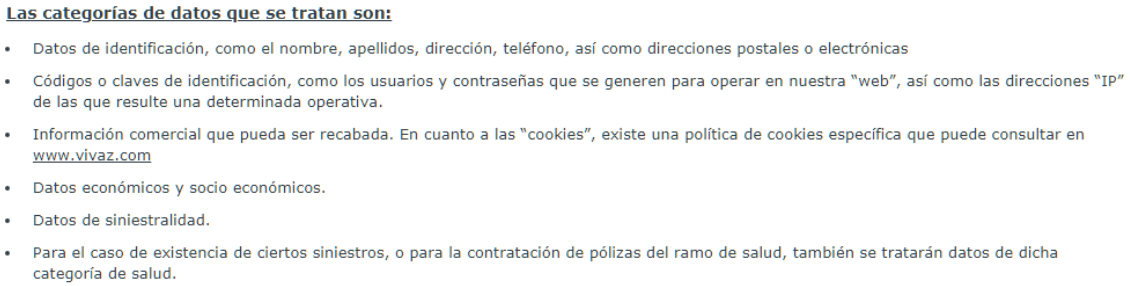


Procedencia:

- La información que manejamos es la que Vd. nos entrega de su persona, o de terceros de los que cuenta con autorización, como serían los menores para los que contrate algún producto, beneficiarios, asegurados no tomadores, o terceros involucrados en un siniestro. A estos datos se unirán los generados posteriormente a lo largo de la vigencia de la Póliza.
- Para poder fijar la prima del seguro al menor importe posible, así como para contrastar y completar sus datos, la ley nos permite acceder y completar su información con distintas bases de datos legalmente accesibles, en función de finalidades legítimas, procedentes de ficheros titularidad de terceras entidades, como el Catastro, ficheros de la Dirección General de Tráfico, fichero SINCO, ficheros de solvencia patrimonial y crédito así como ficheros con datos externos estadísticos, todos ellos disponibles sin restricciones. Del mismo modo, en ciertos casos, pueden actualizarse los datos con datos que haya hecho manifiestamente públicos, como los perfiles abiertos de redes sociales.

Imagen 13. Clausula procedencia de la aseguradora Vivaz. Fuente: Vivaz. Línea Directa.

Respecto a los tipos de datos y categorías de datos.



Las categorías de datos que se tratan son:

- Datos de identificación, como el nombre, apellidos, dirección, teléfono, así como direcciones postales o electrónicas
- Códigos o claves de identificación, como los usuarios y contraseñas que se generen para operar en nuestra "web", así como las direcciones "IP" de las que resulte una determinada operativa.
- Información comercial que pueda ser recabada. En cuanto a las "cookies", existe una política de cookies específica que puede consultar en www.vivaz.com
- Datos económicos y socio económicos.
- Datos de siniestralidad.
- Para el caso de existencia de ciertos siniestros, o para la contratación de pólizas del ramo de salud, también se tratarán datos de dicha categoría de salud.

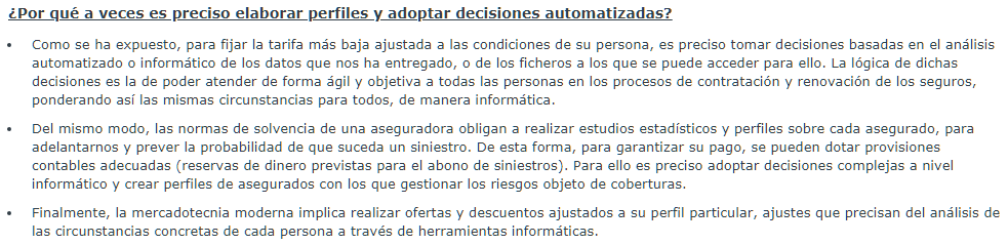
Imagen 14. Clausula informativa respecto a las categoría de datos de la aseguradora Vivaz. Fuente: Vivaz. Línea Directa.

Desde mi punto de vista, aunque no responda a la política de marketing de la empresa, convendría destacar y puntualizar que los datos más sensibles y delicados que se recogen son los de categoría de salud. Convendría expresas qué medidas de seguridad técnicas y organizativas se realizan. No hay que olvidar que el legislador, a priori, mantiene que los datos de categoría especial están prohibidos ser tratados (art. 9.1 RGPD) salvo las excepciones expresas (art. 9.2. RGPD). ¿Cuáles son ésas para permitir a la aseguradora el tratamiento? A mi modo de ver, el registro de actividad debería estar en formato electrónico (Art. 30.2 RGPD) a disposición del público con esta información visible para cumplir con el principio de transparencia y responsabilidad activa, más si cabe.

Respecto a los eventuales tratamientos automatizados.

El art. 13. 2. f señala que "la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado". La aseguradora

explica de forma breve y clara la relevancia por el que se realizan estas decisiones automatizadas; “para fijar la tarifa más baja ajustada a las condiciones de su persona…”.

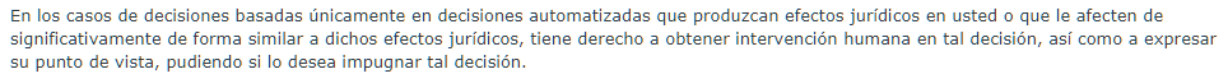


¿Por qué a veces es preciso elaborar perfiles y adoptar decisiones automatizadas?

- Como se ha expuesto, para fijar la tarifa más baja ajustada a las condiciones de su persona, es preciso tomar decisiones basadas en el análisis automatizado o informático de los datos que nos ha entregado, o de los ficheros a los que se puede acceder para ello. La lógica de dichas decisiones es la de poder atender de forma ágil y objetiva a todas las personas en los procesos de contratación y renovación de los seguros, ponderando así las mismas circunstancias para todos, de manera informática.
- Del mismo modo, las normas de solvencia de una aseguradora obligan a realizar estudios estadísticos y perfiles sobre cada asegurado, para adelantarnos y prever la probabilidad de que suceda un siniestro. De esta forma, para garantizar su pago, se pueden dotar provisiones contables adecuadas (reservas de dinero previstas para el abono de siniestros). Para ello es preciso adoptar decisiones complejas a nivel informático y crear perfiles de asegurados con los que gestionar los riesgos objeto de coberturas.
- Finalmente, la mercadotecnia moderna implica realizar ofertas y descuentos ajustados a su perfil particular, ajustes que precisan del análisis de las circunstancias concretas de cada persona a través de herramientas informáticas.

Imagen 15. Clausula informativa respecto a perfiles y decisiones automatizadas de la aseguradora Vivaz. Fuente: Vivaz. Línea Directa.

Pero ahora bien, el derecho a la oposición (“y al derecho de intervención humana”) de estos tratamientos debe ser claro e informado al potencial asegurado. Y así lo realiza:



En los casos de decisiones basadas únicamente en decisiones automatizadas que produzcan efectos jurídicos en usted o que le afecten de significativamente de forma similar a dichos efectos jurídicos, tiene derecho a obtener intervención humana en tal decisión, así como a expresar su punto de vista, pudiendo si lo desea impugnar tal decisión.

Imagen 16. Clausula informativa respecto al derecho de oposición en perfiles y decisiones automatizadas de la aseguradora Vivaz. Fuente: Vivaz. Línea Directa.

No obstante, nos planteamos cuestiones como ; ¿de qué manera se debe justificar y hasta qué punto llegar con dicha justificación? ¿deberán explicar los “árboles de decisión” que posibilitan la “ruta de aprendizaje” y cómo?

5. CONCLUSIONES

La industria del cuidado de la salud aprovechará al máximo la revolución digital lo que se traducirá en ciertas repercusiones y perspectivas de futuro. En concreto, a mi modo de ver, las *compañías farmacéuticas* no podrán controlar totalmente los datos generados (su activo

más valioso) de sus productos o servicios, salvo que interactúen con terceros (pacientes, investigadores, profesionales sanitarios, empresas tecnológicas, universidades, etc.), algo que podrán realizar solo en el contexto de transformación digital.

Por otro lado, se encuentran *las aseguradoras (interactivas o virtuales, también)* que *s*eguirán otorgando incentivos o recompensas a las personas que utilicen ciertos dispositivos y ceden sus datos personales. Este es un escenario que despierta gran preocupación por varios motivos a mi modo de ver

Cuando se trata de seguros interactivos que establece el carácter obligatorio del uso de dispositivos como wearables o apps para el seguimiento y estudio de la condición física y la rentabilidad de los clientes potenciales, se requerirá extremar enormemente las precauciones y la transparencia en la información del alcance del tratamiento de datos y justificar, el empleo de dispositivos siendo proporcional y minimizando los datos necesarios, cumpliendo las obligaciones correspondientes en materia de protección de datos. Es una cuestión absolutamente delicada que requerirá no perder de vista en el futuro de las aseguradoras interactivas con convenios con tecnológicas.

CAPÍTULO II. ALGUNAS CONSIDERACIONES ESPECÍFICAS SOBRE LAS TECNOLOGÍAS APLICADAS A LA INDUSTRIA DEL CUIDADO DE LA SALUD DIGITAL

SUMARIO: 1. CLOUD COMPUTING DE LA SALUD.- 1.1.Introducción. 1.2.Riesgos y la protección de datos. 1.3.Una aproximación a las posibles soluciones. 2. INTERNET DE LAS COSAS DE SALUD.- 2.1.Introducción. 2.2.Clasificación del IoT de la salud. 2.3.Riesgos y la protección de datos. 2.4.Una aproximación a las soluciones posibles. 3. BIG DATA DE LA SALUD. 3.1.Introducción. 3.2.Riesgos y la protección de datos. 3.3.Una aproximación a las posibles soluciones. 3.4.Fases del proyecto big data aplicado al cuidado de la salud. 4. INTELIGENCIA ARTIFICIAL Y MACHINE LEARNING DE LA SALUD.- 5. BLOCKCHAIN Y DLT EN SALUD. 5.1.Introducción. 5.2.Clasificación de Blockchain. 5.3.Aplicabilidad a la Atención Sanitaria: utilidades y casos reales. 5.4.Aplicabilidad a la Industria Farmacéutica: utilidades y casos reales. 5.5.Aplicabilidad en la Industria Aseguradora: utilidades y casos reales. 5.6.Fases del proyecto blockchain aplicado al cuidado de la salud. 5.7.Contexto futuro.

"The future is not to be predicted, it is to be created"

(Stefan Hyttfors, 2016)

1. CLOUD COMPUTING DE LA SALUD.

1.1. Introducción.

Las primeras manifestaciones se pudieron encontrar en los cajeros automáticos de los bancos, extendiéndose sobre todo en los años 80 donde se permitía que el usuario pudiera interactuar en red con su banco desde cualquier terminal. El concepto "*cloud computing*" fue atribuible a *George Gilder*, quien en el 2006 publicó en la revista *Wired* el artículo "*The Information Factories"* donde por primera vez se mencionaría a esta tecnología.

MARTÍN MIRALLES (2010,16)[134] establece "en el momento en el que la nube deja de ser exclusivamente un medio de transporte de la información, para pasar a tener

[134] Miralles, R. (dic. 2010). Cloud computing y protección de datos. En VI Congreso Internet, Derecho y Política. Cloud computing: El derecho y la política suben a la nube". (Monográfico en línea). *IDP*.

capacidad de procesamiento de la información, se le añade el término *computing;* a pesar de que en realidad la capacidad de procesamiento no recae exactamente en la nube, sino en aplicaciones, plataformas e infraestructuras disponibles en la Red y de que, en algunos aspectos, se comportan como los dispositivos de la nube a la que he hecho referencia."

El NIST especifica que; "cloud es un modelo que permite acceso remoto, según nuestras necesidades y bajo demanda, y a través de una red de comunicaciones, a un conjunto compartido de recursos de cómputo configurables (redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser reservados y liberados de manera rápida con un mínimo esfuerzo e intervención por parte del proveedor"

A priori, desde el punto de vista tecnológico hay que tener presenta las siguientes consideraciones y características :

i. la *virtualización* es una característica tecnológica esencial de *cloud* que oculta la complejidad tecnológica al usuario y permite una mayor flexibilidad facilitando el uso y su independencia;
ii. la *multitenencia* donde la opción de "multi-alquiler" implica una gran cantidad de posibles problemas en la materia que nos centra; la protección de datos;
iii. la *privacidad* junto con la *seguridad y compliance* son obviamente esenciales en todos los sistemas *cloud* al tratar con datos y códigos potencialmente sensibles. El 95% de los empresarios en España cree que no son responsables de la seguridad de los datos cuando éstos están almacenados en la nube.
iv. la *gestión de datos* también lo es, sobre todo en cloud como almacenamiento;
v. Las *APIs y / o mejoras de programación* donde es el usuario quien puede encargarse de la programación y mejora cuando antes era el desarrollador.

Por su parte, la Comisión Europea (2010) señala necesario tener en cuenta son los siguientes *aspectos no funcionales*[135][136]:

Revista de los Estudios de Derecho y Ciencia Política. N.11. UOC. Recuperado de http://idp.uoc.edu/ojs/index.php/idp/article/view/n11-miralles/n11-miralles-esp%3E ISSN 1699-8154

[135] Comisión Europea, *The Future of Cloud Computing. Opportunities for European cloud computing beyond.* Recuperado de http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf

[136] Y por supuesto, no olvidemos el *punto de vista económico*. Según el Grupo de Trabajo de la Comisión Europea cabe mencionar los siguientes elementos: (i) La *reducción de costes* es una de las primeras preocupaciones para construir un sistema *cloud* que pueden adaptarse a los cambios, al comportamiento del consumidor y reducir el costo de mantenimiento de la infraestructura y adquisición. ; (ii) *El pago por uso.* La capacidad de acumulación de costes de acuerdo con el consumo real de los recursos es una característica relevante de los sistemas *cloud*. Al pasar del modelo de inversión de capital inicial habitual a un gasto por uso, *cloud* permite que las PYME y empresarios puedan acelerar el desarrollo y adoptar soluciones innovadoras; (iii) *Mejora el tiempo de salida al mercado* ya que es importante sobre todo para las PYME, que pueden vender sus servicios de forma rápida; (iv) *Retorno de la inversión* es esencial para

i. La *elasticidad* es una característica esencial de los sistemas *cloud* y tiene que ver con la capacidad de la infraestructura para adaptarse a los cambios, requisitos potencialmente no funcionales. Gracias a ello, se pueden almacenar gran tamaño de datos y puede haber bastantes usuario simultáneos, etc. .

ii. La *fiabilidad*[137] es esencial, también. Ésta indica la capacidad de garantizar un funcionamiento constante del sistema sin interrupción, es decir, sin pérdida de datos, no hay código de reinicio durante la ejecución, etc. En particular, hay una fuerte relación entre la disponibilidad y fiabilidad, sin embargo, la fiabilidad se centra en la prevención de la pérdida de datos.

iii. La *calidad de* servicio de soporte debe cumplirse cuando se externalizan estos servicios. Las métricas de calidad básicas pueden ser el tiempo de respuesta, el rendimiento, etc.

iv. La *agilidad y la adaptabilidad* son también características esenciales de los sistemas *cloud* que se relacionan íntimamente con la elasticidad. Incluye la reacción al tiempo en los cambios (cantidad de solicitudes, tamaño de los recursos) o la adaptación a los cambios en las *condiciones ambientales* que, por ejemplo, requieren de diferentes tipos de recursos, de calidad o de rutas.

v. La *disponibilidad de servicios y datos* se encuentra en la capacidad de introducir redundancia para los servicios de datos.

1.2. Riesgos y la protección de datos

Analicémoslos detenidamente a continuación:

i. *Falta de control del cliente cloud.* La pérdida de control y gobierno por parte del cliente cloud podría dar lugar a la imposibilidad de cumplir con los requisitos de seguridad, a la falta de confidencialidad, integridad y disponibilidad de los datos. Cuando decimos que hay preocupación por el control nos referimos a que los clientes, actualmente, no tienen el *poder de decisión* de *dónde se almacenan sus datos,* ni tampoco sus proveedores les brindan suficiente transparencia. Por lo general, podemos decir que los datos pasan a situarse en algún lugar indeterminado y variable. Es por ello que hoy en día existen reticencias a las

---

todos los inversores y no siempre se puede garantizar, de hecho algunos sistemas de nubes actualmente no cumplen con este aspecto. El empleo de un sistema *cloud* debe asegurar que el coste y el esfuerzo invertido en él se vea compensado por sus beneficios; (v) Los *gastos serán operativos y* en función de las necesidades; (vi) *"Going Green"* es relevante no sólo al reducir los costes adicionales de consumo de energía, sino también por reducir la "huella de carbono".

[137] Del Valle, M, (2014) La computación en la nube en Europa y en España: una oportunidad de negocio. Folleto *DELL EMC*. Recuperado de https://www.dellemc.com/es-es/solutions/storage/ecs/cloud-services-simple-storage.htm (La autora señala que en un informe de *Verizon* y *Emc* se incluyen que las principales barreras en Europa para la adopción del *cloud computing* son la seguridad y protección de datos (30%), la confiabilidad (25%) y la localización de los datos (24%). Las principales preocupaciones de los clientes tienen que ver sobre todo con los siguientes interrogantes: "¿Quién es responsable de mis datos y de su integridad?; ¿qué pasará si ocurre una brecha en la seguridad?; ¿es fácil cambiar mis datos a otro proveedor en la nube, o conectar con otra aplicación de otro proveedor"?)

grandes empresas tecnológicas estadounidenses que ofrecen servicios en la nube como *Amazon Web Services* (*AWS*), *Windows Azure, Google App Engine, Google Cloud Platform*[138]. La mejor manifestación de la pérdida de control estará en los conocidos *Clicks-Through* o de adhesión y resulta ser el procedimiento habitual para formalizar la activación de una relación contractual entre usuario –mayoritariamente PYME o persona física- y el proveedor *cloud*[139].

ii. *Falta de transparencia en la gestión del proveedor de servicios.* Nos referimos sobre todo a la posible existencia de la cadena de procesamiento de datos por *múltiples procesadores y subcontratistas.* Es necesario que los usuarios cuyos datos personales estén siendo procesados en la nube sean informados acerca de la identidad del responsable del tratamiento y el propósito del procesamiento de los mismos tal y como establece la normativa. Pero la realidad es que los proveedores no siempre proporcionan a los usuarios finales las herramientas necesarias al de tratamiento en la gestión de los datos (acceso, destrucción, portabilidad)

iii. *Posibles conflictos de intereses* debido a que los proveedores procesan datos provenientes de diferente fuentes. Por ejemplo, el proveedor cloud puede servirse del privilegio de vincular información de distintos clientes para su interés y sin el consentimiento de los titulares.

1.3. Una aproximación a las posibles soluciones

[138] Así por ejemplo, la autoridad de control de Suecia prohibió el uso de *Google App Engine* ya que no proporcionaba suficiente información sobre cómo "manejar" los datos, cuánto tiempo se mantenían, quién accede a ello...etc.

[139] Vid. Kuan Hon, W., Millard, C. Walden, I. (2012) . Negotiating cloud contracts: Looking at clouds from both sides now. *Standford Technology Law Review.* Vol. 16. Number 1.. Recuperado de http://stlr.stanford.edu/pdf/cloudcontracts.pdf. (Según los autores, muchos de los clientes *cloud* declararon que sus proveedores -incluso de los más grandes- no tenían recursos jurídicos internos suficientes para hacer frente a solicitudes de los usuarios y modificar los términos de contratación. Tampoco resulta desconocido por las empresas clientes, descubrir que sus empleados han contratado *cloud* en condiciones estándar y luego traten de negociar con condiciones mejores. Los empleados de las organizaciones no siempre tienen en cuenta los *procedimientos internos de contratación* -sobre todo cuando se tratan de servicios gratuitos-, "gratuito no significa libre de riesgo o libre de extras esenciales").

Como establece *Kuan Hon*[140], sería esenciales algunos elementos para poder enfrentarnos a la nueva protección de datos:

- *multidisciplinariedad entre t*ecnólogos y juristas (binary vs analogue), donde el tecnólogo conozco la terminología de "protección de datos";
- *legislación basada en la evidencia y en la experiencia* (asociaciones profesionales de expertos: ENISA, CSA, Eurocloud, ISMS Forum,etc.);
- *empoderar* a los *reguladores* por medio de "educación" en seguridad;
- enfoque basado desde el *riesgo*;
- apoyar el *intercambio entre gobiernos y organizaciones empresariales*.

A continuación, señalamos una relación de posibles soluciones consistentes en primer lugar, la aplicación de la protección de datos aplicada al tipo de servicio cloud, en segundo lugar a la aplicación del principio de privacidad desde el diseño, y en tercer lugar, la más disruptiva, prometedora y efectiva, el uso de *blockcloud* a través de Blockchain.

i. A través de medidas según tipo de servicio cloud.

Lo más adecuado sería especificar la protección de datos en función del tipo de servicio cloud puesto que las particularidades de los servicios cambian en función del tipo de servicio.

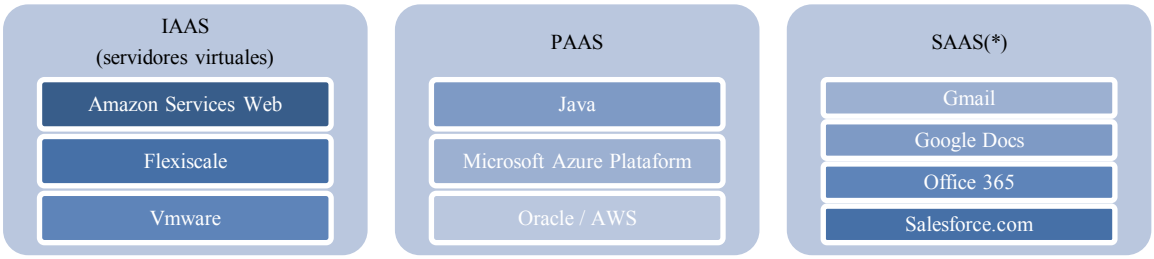


Tabla 9. Ejemplos de Servicios Cloud.

Por ejemplo, con los servicios SaaS[141] (*) es bastante frecuente perder de vista la importancia de las condiciones contractuales de privacidad dado el carácter gratuito del mismo.

[140] Hon, K. (16 de junio de 2015). Cloud Security under the Data Protection Directive and Draft General Data Protection Regulation. En *ENISA EU28 Cloud Security Conference*. Recuperado de https://www.enisa.europa.eu/events/enisa-events/cloud-security-conference-reaching-the-cloud-era-in-the-eu/speakers-images/HonENISACloudSecurityDataProtection-distribution.pdf

[141] Según un estudio de IDC, SaaS representará aproximadamente el 60% del gasto en la nube para 2020. Vid.https://tecnologiaparatuempresa.ituser.es/cloud/2019/02/tendencias-que-influiran-en-el-mercado-saas-en-2019

Respecto a los tipos de nube hemos de señalar las particularidades y riesgos legales de cada una:

a) *Nube pública***.** El proveedor de servicios de *cloud* proporciona sus recursos de forma abierta a entidades heterogéneas. La nube pública es la que encierra mayores problemas dada su naturaleza. En Europa, es donde mayor pérdida de control de los datos se produce por parte del cliente[142].

b) *Nube privada.* Consiste en que una entidad realiza la gestión y administración de sus servicios en la nube para las partes que la forman, sin que en la misma puedan participar entidades externas y manteniendo el control sobre ella. Al pagar los costes, existe mayor margen de negociación por parte del cliente y en consecuencia se pueden mitigar los riesgos*, a priori.*

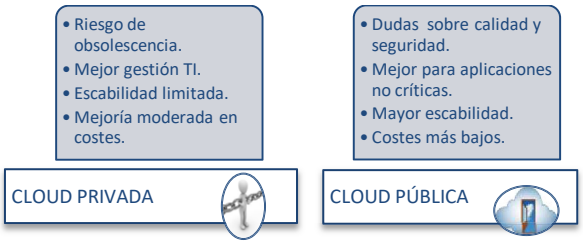


Tabla 10. Características de Cloud privada y pública.

c) *Nube híbrida.* Determinados servicios se ofrecen de forma pública y otros de forma privada. En la actualidad es la que más éxito está teniendo ya que además ayuda a la transformación digital de las empresas.

d.) *Nube comunitaria*. La infraestructura de esta nube es compartida por varias organizaciones y apoya las preocupaciones de una comunidad particular sobre un tema específico, por ejemplo, seguridad, investigación, políticas o cumplimientos. Cuenta con los mismos problemas que la nube pública.

ii. A través de privacidad desde el diseño ("privacy by design").

Empresas proveedoras cloud pueden encontrar una solución a los riesgos de privacidad en el principio de privacidad desde el diseño, como es el caso de *Microsoft.* Una de las herramientas para aplicarlo es el *SDL* (con 7 fases[143]) como proceso de desarrollo de software que ayuda a los desarrolladores a crear *software de seguridad* dirigido para cumplir requisitos de de la *privacidad*. Otra herramienta es *MPS* que son normas que definen prácticas de privacidad y seguridad. Ayuda a minimizar vulnerabilidades en el código de software, protegiendo los datos contra infracciones, y ayuda a asegurar

[142] Vid. en : http://www.computerworld.es/pubs/cw1336/files/35.html
[143] Donde se incluyen la formación de promotores y los directores de programas en los conceptos fundamentales, la construcción *de software seguro que protege la privacidad,* y la respuesta a incidentes de seguridad y *privacidad* cuando se producen.

"desde el principio" que los desarrolladores consideren el factor de la privacidad en todos los productos y servicios *cloud*.

iii. A través de "Blockcloud": la combinación de Blockchain y cloud computing.

Con Blockchain (y DLT) no hay una autoridad centralizada que sea responsable más bien los participantes (partes) múltiples llegan a un consenso registrado en el libro mayor. En esta cadena de bloques se otorga *trazabilidad* a la nube y las entidades que utilizan o administran la nube serían las responsables de sus acciones e *inmutabilidad*. Blockchain podrá demostrar la existencia de un contrato entre el titular de los datos y el proveedor cloud, así como la existencia de los datos en cuestión. Se proporcionarán pruebas claras de las transacciones ya que no será necesario que las empresas registren de forma manual los intercambios lo que genera una mayor confianza[144].

2. INTERNET DE LAS COSAS DE LA SALUD.

Un estudio de Gartner dice que en el año 2020, el *ser humano va a ser un nodo activo de la red IP*. También se espera que a mediado plazo, 14 trillones los dispositivos estarán conectados a alguna red IP.

En 2015, en el *Mobile World Congress*[145] ya se vaticinó que el futuro de la medicina estaría en el Internet de las Cosas, presentándose el *"teddy the guardian"*[146], un osito de peluche, que permitirá medir su temperatura, ritmo cardíaco y nivel de oxígeno en sangre, el cual ya se está probando en hospitales de Reino Unido.

Imagen 17. Teddy the guardian. Fuente: MobyHealthNews

[144]Vid.https://www.revistacloudcomputing.com/2018/10/blockchain-al-servicio-de-un-nuevo-mercado-de-almacenamiento/. (Se trata de un modelo disruptivo que posiblemente requiera de un cambio de mentalidad en los negocios dejando atrás la idea de que el mejor almacenamiento es el centralizado.
[145] Ver en : http://mobileworldcapital.com/es/el-futuro-de-la-medicina-esta-en-el-internet-de-las-cosas/)
[146] Ver en : https://youtu.be/9ydWI3D2KWM Teddy the guardian,

Y también existen soluciones como los *botes de pastillas conectados* para los periodos post hospitalarios que envían datos sobre qué cantidad de medicamentos está ingiriendo un paciente. Los *wearables* permitirán en esos periodos de alta hospitalaria el seguimiento y la alerta al médico en caso de que los pacientes tengan arritmias o primeros síntomas de problemas cardíacos.

En el sector privado, *British Airways*[147] registró una patente de pastilla con varios sensores dirigida a pasajeros, la cual permitiría registrar variables para averiguar si un viajero tiene hambre, frío o en qué fase del sueño se encuentra. Esa información podría ser utilizada para ajustar, por ejemplo, el momento en que se debe servir la comida, parámetros como la luz y temperatura de la cabina, ofrecer una manta, etc.

El esquema de modelo mundial del IoT se podría resumir en estos siete niveles:

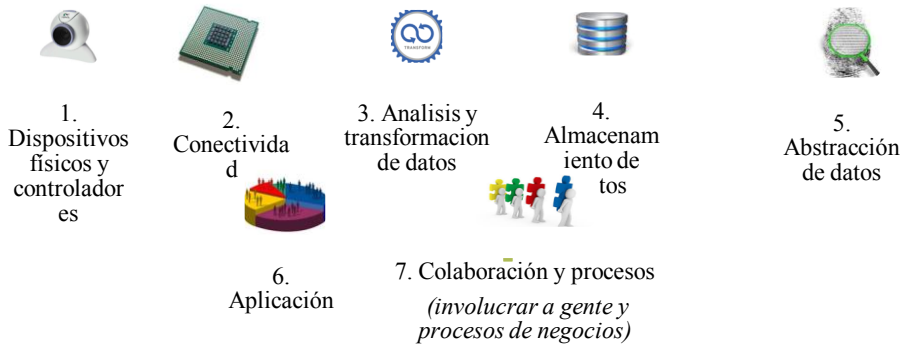


Imagen 18. Esquema del modelo IoT y sus niveles. Fuente: propia.

2.1. Introducción

La primera vez que se utilizó el concepto Internet de las Cosas (*IoT*) fue hace casi dos décadas *por Kevin Ashton* en una presentación en la cual ya estableció que cambiaría el mundo igual que lo hizo Internet. El lo definió*:*

> "Internet de las cosas significa sensores conectados a Internet que se comportan de una forma en donde Internet hace conexiones abiertas ad-hoc intercambiando datos libremente. Esto permite crear aplicaciones inesperadas y un sistema nervioso para el planeta…"

[147] Trenholm, R. (30 de noviembre de 2016). Lucha contra el jet-lag: la píldora digital le dice a la tripulación de cabina lo que necesitas. *CNET*. Recuperado de https://www.cnet.com/news/fight-jet-lag-with-the-digital-pill-that-tells-cabin-crew-what-you-need/

No obstante, el origen al IoT lo encontrábamos en la década de los 80 y no es hasta mediados de los 2000 con las etiquetas RFID cuando se utiliza en comercio o en el rastreo de mascotas o ganado.

Imagen 19. Etiqueta RFID. Fuente desconocida.

Posiblemente el concepto de IoT es conocido por su vinculación con los *"sensores"* pues la palabra más conocida, pero en el futuro, la palabra que nos vendrá antes en la mente cuando hablemos de *IoT* no será *"sensores"* sino *"personas" o "estilo de vida"*[148].

Para el GT29;

> "IoT es una infraestructura en la cual billones de sensores incorporados en dispositivos cotidianos ("cosas" o "cosas vinculadas a otros objetos") son diseñados para registrar , procesar, almacenar y transferir datos y ya que están asociados con identificadores únicos, interactuar con otros dispositivos o sistemas que utilizan capacidades de red.

Por su parte, la Unión Internacional de Telecomunicaciones (ITU) en el 2015 lo define como;

> "una infraestructura global para la sociedad de la información permitiendo servicios avanzados mediante la interconexión de cosas (físicas y virtuales), basados en la interoperabilidad de las tecnologías de información y comunicación existentes y en evolución".

Llegados a este punto es necesario mencionar el sector de *Internet de atención médica* (*Internet of Medical Things*, IoMT)[149]. El cual, se prevé, que madure ganando autonomía con los dispositivos conectados en casa y con la llegada de los vehículos autónomos inteligentes (ej. para emergencias accidentes de tráfico).

[148] En esta tecnología, las cosas deben ser capaces de recibir y/o transmitir datos de o sobre ellos mismos o sus entornos físicos (incluyendo a personas), y además, deberán llevar a cabo alguna acción como puede ser cambiar el termostato. Algunas cosas sólo pueden sentir, algunas sólo actúan, mientras que otras pueden hacer ambas cosas. Por ejemplo, una bomba de insulina inteligente puede medir niveles de azúcar en la sangre de la persona diabética y regularlo apropiadamente.

[149] IoTH es la colección de dispositivos médicos y aplicaciones que se conectan a sistemas de TI de atención médica a través de redes informáticas en línea. Los dispositivos médicos equipados con *Wi-Fi* permiten la comunicación de *máquina a máquina* que es la base de IoMT y se vinculan a plataformas en la cloud en las que se pueden almacenar y analizar los datos capturados.

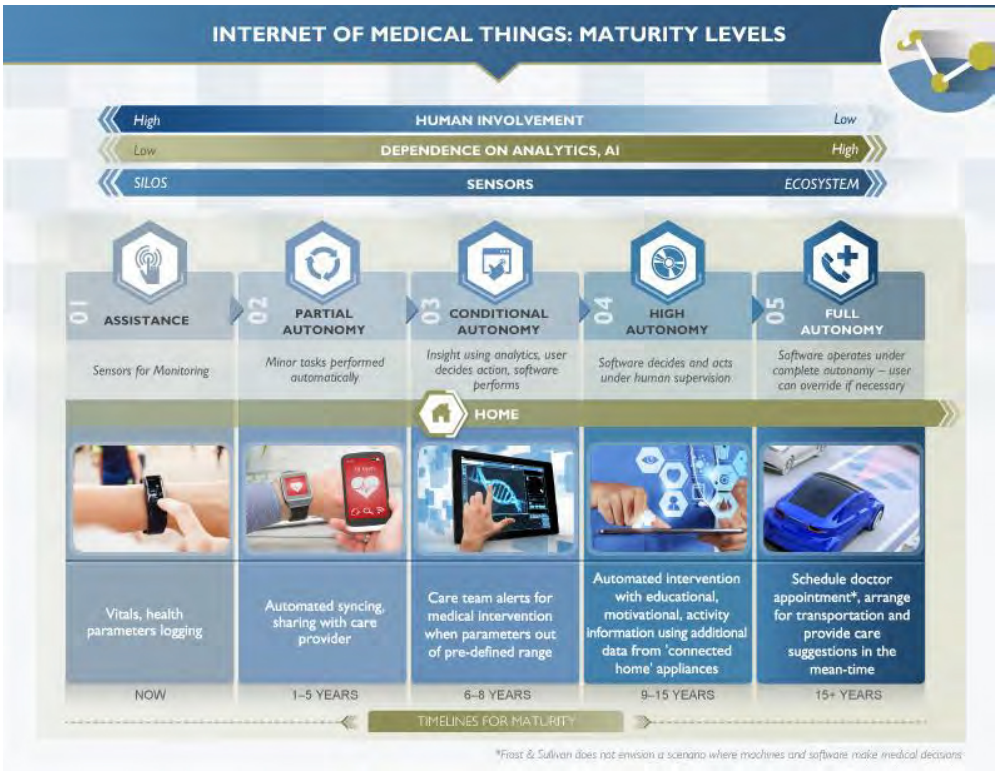


Imagen 20. Niveles de maduración de IoTM. Fuente: Frost & Sullivan[150]

2.2. Clasificación del IoT de la salud

Los investigadores, hace más ocho años, empezaron a mostrar que los sensores de los Smartphone podrían monitorizar a los usuarios e inferir sobre ellos respecto al el estado de ánimo[151] o la progresión de la enfermedad de Parkinson [152] o los patrones de sueño [153]

[150] Frost &Sullivan (27 de junio de 2017). *¿Es IoMT la solución mágica para remodelar la prestación de la atención coordinada y proactiva?* Recuperado de https://ww2.frost.com/news/press-releases/iomt-magic-bullet-reshape-coordinated-and-proactive-care-delivery/

[151] Robert LiKamWa et al., (2011). MoodScope: Building a Mood Sensor from Smartphone Usage Patterns. Recuperado de http://www.ruf.rice.edu/~mobile/publications/likamwa2013mobisys2.pdf. Ver también Robert Likamwa et al. "Can your smartphone infer your mood?" recuperado en http://www.ruf.rice.edu/~mobile/publications/likamwa11phonesense.pdf . (Los autores muestran cómo es el estado de ánimo del usuario a través del smartphone utilizando solo 3 semanas para recoger datos y estadísticas).

[152] Sinziana Mazilu et al., (mayo 2012) "Online Detection of Freezing of Gait with Smartphones and Machine Learning Techniques". En Conference Pervasive Computing Technologies for Healthcare, 2012, 6th International Conference on at San Diego, California. Recuperado de: https://www.researchgate.net/publication/256503573_Online_Detection_of_Freezing_of_Gait_with_Smartphones_and_Machine_Learning_Techniques. (Los autores proponen el uso de los sensores internos de los teléfonos inteligentes para corregir, alertar y tratar el congelamiento de la marcha de un usuario causado por la enfermedad de Parkinson).

[153] Zhenyu Chen et al., (2013) "Unobtrusive Sleep Monitoring Using Smartphones". Recuperado de https://ieeexplore.ieee.org/document/6563918. (Los autores crean un modelo (BES) menos intrusivo para monitorizar el sueño, permitiendo que el usuario duerma sin interactuar con el teléfono. Se explotan una recopilación de sugerencias suaves que vinculan la duración del sueño a varios patrones de uso y observaciones ambientales -silencio prolongado y oscuridad-).

de un usuario, prestando especial atención a no excederse en la intrusión de los mismos. Para continuar con el estudio necesitamos abordar los tipos de IoT existentes. El GT29 en su dictamen señalaba esencialmente tres desarrollos específicos: *los dispositivos llevables, los autcuantificables y la domótica.*

i. *Dispositivos llevables ("Wearables").* Pueden integrar cámaras, micrófonos y sensores que permiten grabar , e incluso, transferir los datos al fabricante del dispositivo. Podemos hacer la siguiente clasificación:

a. *Relojes y pulseras inteligentes.* Permiten monitorizar el ritmo cardíaco, los niveles de glucosa, los pasos que se dan durante el día, las horas de sueño durante la noche, las calorías que consume el usuario o monitoriza la presión arterial. Todos estos datos se almacenan y se registran en apps móviles, con las que el paciente puede compartir sus datos con el médico, mejorando el seguimiento y la adherencia al tratamiento. Por ejemplo, es *Embrace***,** desarrollado por el MIT emplea inteligencia artificial para detectar crisis epilépticas y convulsiones en el paciente**,** alertando automáticamente a un profesional sanitario o a la persona designada para socorrerle.

b. *Gafas inteligentes.* Un ejemplo es *MyEye 2.0*[154]**,** que permite a los usuarios mediante inteligencia artificial oír aquello que no pueden ver. El dispositivo lee textos impresos y digitales, reconocer colores, billetes en curso, rostros o nombres de las calles e identifica productos en el supermercado.

c. *Ropa inteligente.* Una Universidad de Washington ha diseñado un tejido inteligente capaz de almacenar datos como códigos de seguridad o de identificación sin necesidad de recurrir a sensores o dispositivos electrónicos a través de RFID. Xiaomi ya ha sacado la camiseta inteligente que hace electrogramas[155].

ii. *Sensores autocuantificadores ("Quantified Self").* Están diseñados para ser llevados regularmente por personas que desean registrar información sobre sus propios hábitos y estilos de vida, sobre su peso, pulso u otros indicadores de salud. Así por ejemplo, los marcadores IP de última generación pueden transmitir datos a través de internet e incluso ser controlados y configurados de forma remota. Los datos de salud que pueden recoger son frecuencias cardiacas o arritmias.

[154] Para más info: https://www.youtube.com/watch?time_continue=5&v=zGolyx3NCBc
[155] Vid. https://hipertextual.com/2019/06/xiaomi-lanza-camiseta-inteligente-con-capacidad-electrocardiogramas

Hay otro ejemplo de sensor autocuantificador, llamado *Breathometer*[156], que funciona como alcoholímetro de bolsillo.

Imagen 21. Breathometer. Fuente: Engadget

Pero no podemos olvidarnos de la importancia que están teniendo los dispositivos como *Fitbit (*conectados a *smartphone)* en la vida de personas no solo para "cuantificar su salud", sino también para servirse de sus informes como pruebas documentales para procedimientos judiciales[157] o para "salvarlas"[158].

iii. *La domótica.* Se le podría añadir a la categoría del sector IoTM en general, o salud automatizada del hogar, en particular. Así por ejemplo, *eBPlatform*[159] es un sistema de *IoT* diseñado para la atención domiciliaria de los pacientes con

[156] Peppet, S.R. (2015) Regulation the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. *Texas Law Review*. Recuperado de http://www.texaslrev.com/wp-content/uploads/2015/08/Peppet-93-1.pdf

[157] Rudner, j, McDougall, C., Sailam, V. Smith, M., Sacchetii, A. (2016) Interrogation of patient smartphone activity tracker to assist arrhythmia management. *Annals of Emergency Medicine*. Recuperado de http://www.annemergmed.com/article/S0196-0644(16)00143-8/fulltext. (Se señala que "actualmente, los rastreadores de actividad no se consideran dispositivos médicos aprobados, y el uso de su información para tomar decisiones médicas es a criterio del médico", no obstante, "el interrogatorio de un rastreador de actividad no solo puede correlacionar los síntomas con las tasas de pulso, *sino también documentar el inicio o la duración de las tasas anormalmente altas o bajas*").

[158] Crawford, K. (nov 2014). When Fitbit Is the Expert Witness. *The Atlantic*. Technology. Recuperado de https://www.theatlantic.com/technology/archive/2014/11/when-fitbit-is-the-expert-witness/382936/. (En 2014, una persona presentó una demanda alegando que ella todavía sufría heridas por un accidente automovilístico producido hace cuatro años. Los abogados del demandante utilizaron sus datos de *Fitbit* analizados por un tercero compañía para corroborar las reclamaciones. Los abogados demandantes para mostrar que sus niveles de actividad son aún más bajos que los valores de referencia para alguien de su edad y que merece una compensación. El experto estadounidense en derecho de privacidad *Kate Crawford* observó que: *"los datos de los wearables podrían ser fácilmente utilizado por las aseguradoras para negar reclamos por incapacidad, o por los fiscales buscando una rica fuente de evidencia incriminatoria"*. En este sentido, el director de *Vivamatica*, el Dr. *Rich Hu*, dijo que las aseguradoras no pueden obligar a los demandantes a usar *Fitbit*, pero pueden solicitar una orden judicial a cualquiera que almacene datos que se puedan usar para lanzarlos. Llegados a este punto, cabe preguntarnos si esto cambiará la relación de las personas con su dispositivo portátil cuando sepan que puede ser una fuente de información en ocasiones, positiva, y en otras, negativa para sus intereses).

[159] Liu, Y, Niu, J., Yang, L., Shu, L. (2014). eBPlatform: An IoT-bases system for NCD patients homecare in China. En *IEEE Global Communications Conference.* Recuperado de http://ieeexplore.ieee.org/document/7037175/?reload=true

enfermedades no transmisibles en China[160]. Y por otro lado, existe un *servicio de medicación inteligente* como la plataforma *iHomeHealth-IoT*[161], conformada por una caja de medicina inteligente (*iMedBox*) y envases farmacéuticos inteligentes (*iMedPack*) con capacidades de comunicación por RFID[162].

Al margen de los tres tipos de IoT destacables por el GT29, el experto *Peppet* (2013, 16-7), señala entre otros a los sensores de contacto íntimo o los ingeribles o implantables. A continuación, desarrollaré ejemplos de los mismos.

iv. *Sensores IoT de contacto íntimo.* Son dispositivos incrustado en vendas, cintas médica, parches o tatuajes[163] usados en la piel y está más orientado a la naturaleza médica que al entretenimiento. Por ejemplo, existen las lentillas inteligentes que sirven para medir la glucosa[164]. Google en 2018, canceló el proyecto que tenía en estudio tras reconocer la dificultad de que la lágrima pueda detectar los niveles de azúcar igual que se hace en sangre.

Imagen 22. Ejemplo de lentilla inteligente. Fuente: Pintarest

[160] Fue utilizado un sensor denominado *eBox*, el cual puede ser desplegado en el hogar del paciente y permite el monitoreo constante de su presión arterial, azúcar en la sangre y señales de electrocardiograma. Los *datos asociados* a las mediciones son desplegados en un portal web en el cual los médicos pueden proporcionar un tratamiento en línea.

[161] Pang, Z., Tian, J., Chen, Q. (2014). Intelligent packaging and intelligent medicine box for medication management towards the Internet-of-Things. En *16th International Conference on Advanced Communication Technology*. Recuperado de http://ieeexplore.ieee.org/document/6779193/

[162] La plataforma es capaz de enviar una alerta al paciente visualizada en la caja inteligente indicando que la hora de la toma del medicamento ha pasado, además esta alerta se complementa con un mensaje de texto al médico a cargo.

[163] Villariño, A. (Andrés Vilariño). (29 de Marzo de 2019). Recuperado de https://twitter.com/andresvilarino/status/1111781345481629696. (Se tratan de tatuajes móviles que detectan exposiciones al sol que pueden ser perjudiciales para la salud).

[164] Vid. https://campussanofi.es/e-patient/noticias/lentillas-inteligentes-para-medir-los-niveles-de-glucosa/

Por ejemplo, el *Raiing Wireless*[165] *es* un sensor de termómetro de contacto *peel-and-stick* que transmite temperatura corporal en tiempo real para el smartphone de un usuario. De manera similar. Por su parte, el parche *Metria* de *Avery Dennison* es un dispositivo de monitoreo médico remoto que mide la temperatura, sueño, frecuencia cardíaca, medidas tomadas y tasas de respiración. Y también existen sensores[166] para las uñas que detectan enfermedades como el Parkinson.

v. *Sensores ingeribles e implantables*[167]. Incluyen "pastillas inteligentes" que contienen diminutos sensores diseñados para monitorear el interior del cuerpo. Por mencionar ejemplos, la *PillCam*[168], una cámara del tamaño de una píldora se usa para *detectar sangrado* y otros problemas en el tracto gastrointestinal, o la *SmartPill-an*[169] que mide la presión, los niveles de pH y la temperatura, la cual viaja a través del cuerpo o, el *Proteus Feedback System*[170] (aprobada por la FDA en 2012), que es una píldora que monitorea glucosa en sangre, presión arterial y función cardíaca. La FDA también ha aprobado la presentación de un medicamento antipsicótico[171] para el tratamiento de algunos cuadros de desórdenes como la esquizofrenia o el trastorno bipolar en la piel. También, en la salud dental, también ha llegado el desarrollo de IoT, por ejemplo, con un *sensor implantado entre los dientes*[172] el cual puede transmitir información de forma inalámbrica a un dentista para evaluar enfermedad dental o hábitos poco saludables o incluso para controlar los nutrientes y otras sustancias que se digieren[173]. Se ha desarrollado también un sistema que permite imprimir

[165] Comstock, J. (16 de noviembre de 2012). FDA aprueba el termómetro corporal con capacidad para Iphone. *Mobihealthnew*s . Recuperado de http://mobihealthnews.com/19110/fda-clears-iphone-enabled-body-thermometer/

[166] Nobbot (3 de enero de 2019). Investigadores de IBM sacan las uñas para luchar contra el Parkinson. *Editorial Nobbot.* Recuperado de https://www.nobbot.com/general/ibm-sensor-de-unas/

[167] Cadie Thompson (2013). The Future of Medicine Means Part Human. Part Computer, *CNBC.* Recuperado en http://www.cnbc.com/id/101293979. (La autora declara que dentro de una década hasta una tercera parte de la población de EE. UU. tendrá un dispositivo implantable temporal o permanente dentro de su cuerpo).

[168] Vid. http://www.givenimaging.com/enus/Innovative-Solutions/Capsule-Endoscopy/Pages/default.aspx

[169] Vid. http://givenimaging.com/en-us/InnovativeSolutions/Motility/SmartPill/Pages/default.aspx

[170] Vid. http://www.proteus.com/ technology/digital-health-feedback-system/

[171] Dans. E. (2017). Devorando sensores: el futuro de la medicina. Recuperado de https://www.enriquedans.com/2017/11/devorando-sensores-el-futuro-de-la-medicina.html

[172] Ross Brooks (2013) Tooth-Embedded Sensor Relays Eating Habits to the Dentist, *PSFK* http://www.psfk.com/2013/07/tooth-sensor-track-eating-habits.html

[173] Nobbot (3 de enero de 2019). Investigadores de IBM sacan las uñas para luchar contra el parkinson. *Editorial Nobbot*. https://www.nobbot.com/general/sensor-diente-rastrea-comida/

dispositivos[174] (ver imagen inferior) y de esta manera poder monitorizar funciones del organismo o incluso administrar fármacos a través de ella.

Imagen 23. Ejemplo de tatuaje inteligente impreso.

Por su parte, *Skin electronics desarrollado* en la Universidad de Tokyo es otro ejemplo de lo que está por venir en materia de piel artificial electrónica.

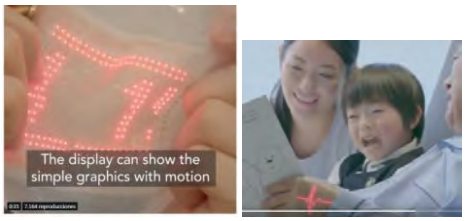


Imagen 24. Ejemplo de piel inteligente Fuente: Universidad Tokio. Gigadgets[175]

En la Universidad de *Maryland*[176], llegan más lejos, con los chipsubcutáneos, los cuales no sólo detectarán enfermedades sino que otorgarán respuesta médica. Para el Investigador *William Bentley*, además de conseguir información biológica molecular en un dispositivo y trasmitirlo a través de un interfaz, lo interesante sería hacer una *transmisión reversa*, donde se pudiera activar a la biología por medio de electrodos[177].

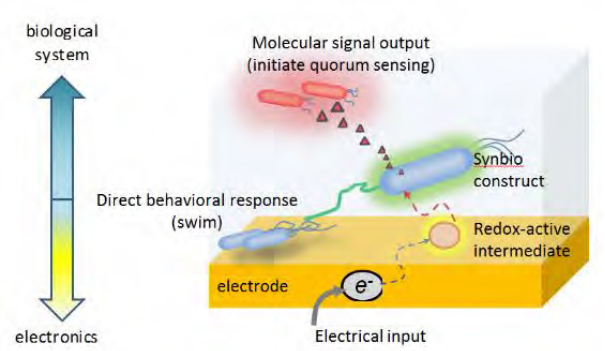


Imagen 25. Ejemplo de transmisión reversa de datos de salud. Fuente: Universidad de *Mayland*[178]

[174] Ver en https://youtu.be/DTXqUrmr3FQ
[175] Villariño, A. (29 de marzo de 2019) Recuperado de https://twitter.com/andresvilarino/status/1111694528438771712. "This Futuristic #ESkin Can Monitor Your #Health Remotely. via @DigitalMedDoc"
[176] Ver en http://www.bioe.umd.edu/news/news_story.php?id=10234
[177] Los investigadores creen que sí es posible y lo han demostrado con células bacterianas, comprobando que los impulsos electrónicos pueden cambiar el comportamiento de las células. De hecho, las señales eléctricas enviadas a través de las moléculas han demostrado que se podrían *controlar el consumo de glucosa y regular la actividad enzimática.*
[178] Recuperado de http://www.bioe.umd.edu/sites/default/files/images/011717-figure.jpg

Piénsese en el caso de los pacientes o usuarios diabéticos regulando la actividad enzimática. Otra alternativa de *transmisión reversa* se podría dar gracias a las *píldoras inteligentes* con un sistema microelectrónico que pueda registrar patógenos en el aparato digestivo, las cuales liberarían algún tipo de medicamento para combatirlo regulable por el paciente.

2.3. Riesgos y la protección de datos.

Los dispositivos de la *IoT* de consumo introducen nuevas tecnologías, nuevas técnicas de recopilación de datos, nuevos flujos de información y nuevas partes interesadas *(piénsese en el proveedor de servicios de salud, el laboratorio, el paciente, el dispositivo médico y la compañía de seguros).*

A priori, conviene señalar lo que establece el *Dictamen emitido el día 1º de julio de 2012, por el GT29*, acerca de los riesgos que acarrear los *dispositivos inteligentes*:

> "…La *fragmentación de los numerosos actores que intervienen* en el desarrollo de aplicaciones también supone un riesgo grave para la protección de datos. Un determinado dato puede ser transmitido, en tiempo real, desde el dispositivo para ser procesado en cualquier parte del planeta o ser copiado entre cadenas de terceras partes…". "Los principales riesgos para la protección de los datos de los usuarios finales son la falta *de transparencia y conocimiento de los tipos de tratamiento* que las aplicaciones pueden realizar, combinada con la *falta de consentimiento significativo* por parte de los usuarios finales antes de que se produzca el tratamiento de datos. Las *insuficientes medidas de seguridad*[179] la clara tendencia hacia la *maximización de los datos* y la elasticidad de los fines para los que se recogen datos personales también contribuyen a los riesgos …

Ahora bien, ¿cuáles son los posibles *riesgos y soluciones* en materia de privacidad de los IoT de salud? Adelantamos el siguiente cuadro:

	Problemas	**Soluciones**
i.	Discriminación y sesgos.	Modelo autogestión de la privacidad y transparencia.
ii.	Problemas de ciberseguridad y reidentificación.	Medidas de seguridad técnicas y organizativas obligatorias; anonimización irreversible (RGPD), datos

[179] La empresa americana *WeVibe* ha sido demandada en el Tribunal Federal de Chicago en el que por recabar información confidencial e íntima -como la temperatura- a través de los dispositivos *wareables inteligentes* (juguetes sexuales vibradores) sin que los consumidores fueran conocedores. La empresa guardaba los datos enlazándolos con el nombre de la persona que los había adquirido. Para evitar mayor repercusión social llegaron a un acuerdo de casi 4 millones de dólares para el grupo de consumidores afectados. Recuperado de https://www.eleconomista.es/empresas-finanzas/noticias/8224842/03/17/Cuando-los-vibradores-te-espian-multa-de-4-millones-a-una-empresa-que-registraba-el-uso-de-sus-consoladores.html

		agregados. Blockchain
iii.	Numerosos actores y falta de control de gestión legitimación del tratamiento	Contratos de encargo de tratamiento y subencargo según RGPD, adhesión a códigos de conducta, certificación ISO/IEC 30141. Blockchain.
iv.	Maximización de datos personales	Principio de minimización obligatorio en RGPD

Tabla 11. Problemas y soluciones en materia de privacidad en IoT

A continuación, procedemos a desarrollarlos;

i. *La discriminación y los sesgos*[180]. Los Smartphone están recopilando datos sobre el comportamiento de los individuos y estos datos son tan granulares y de alta calidad que permiten a menudo inferencias en las personas. Pongamos un ejemplo, un consumidor de *Fitbit Fitness* puede controlar su estado físico y salud general almacenándolos en la web de Fitbit, y a la vez su uso podría repercutir en su búsqueda de empleo[181], en su actual relación laboral[182] o en la solicitud de póliza de seguro[183].

[180] *Heather M. Patterson* (ver http://www.heatherpatterson.org/) ha observado que la escala, el alcance y los flujos no tradicionales de información de salud, junto con sofisticadas técnicas de minería de datos que apoyan inferencias de salud confiables, *ponen a los consumidores en riesgo de discriminación en el terreno laboral, en al amito de seguros o en el marketing conductual no deseado*. Según la autora, la legislación estadounidense en materia de privacidad abarcaría a los dispositivos de IoT médicos que se utilicen para el tratamiento médico, pero *no para los wearables de fitness, autodispositivos cuantificados, detectores de sueño, y cualquier otro objeto que rastree datos biométricos, signos vitales u otros la información de salud utilizada para interés personal*. Para ella, un área de preocupación es la de las compañías de seguros que usan la aptitud de *seguimiento automático y la información de salud* contra sus *clientes, negando reclamaciones por lesiones.* Según la autora, hay un estudio en EE. UU. (Ackerman, L. 2013. Mobile Health and Fitness Applications and Information Privacy. Recuperado de http://bit.ly/2dhGc89) en términos de las aplicaciones móviles gratuitas de salud y estado físico que señala lo siguiente: *El 26% de las aplicaciones gratuitas y el 40% de las aplicaciones de pago no tenían una política de privacidad. El 39% de las aplicaciones gratuitas y el 30% de las aplicaciones pagas enviaron datos a alguien no divulgado en la aplicación o la política de privacidad. Y solo el 13% de las aplicaciones gratuitas y el 10% de las aplicaciones pagadas cifraron todas transmisiones de datos entre la aplicación y el sitio web del desarrollador.*

[181] Como dice Peppet (2013), los datos de Fitbit podrían revelar mucho a un empleador como la impulsividad y la incapacidad para retrasar la gratificación, los hábitos de ejercicio - que se correlacionan con el abuso de alcohol y drogas-, trastornos de la alimentación, comportamiento, cigarrillos fumados, deuda de tarjetas de crédito. Estas informaciones podrían determinar la contratación o el descarte del candidato a un puesto de trabajo.

[182] Ver en https://globalchallenge.virginpulse.com/. (La empresa *Virgin Pulse* por ejemplo, como consultoría de implantación de programas eHealth para trabajadores utiliza básicamente medidores de dispositivos IoT. El desafío estará en mantener protegida la información de los empleadores).

[183] Pensemos un ejemplo. Un empleador o una aseguradora accede a los datos revelados de un acelerómetro y un giroscopio. Ver Kaivan Karimi (2013) "The role of sensor fusion and remote emotive computing (REC) in the IoT". Recuperado de https://cache.freescale.com/files/32bit/doc/white_paper/SENFEIOTLFWP.pdf. (Ambos aparatos IoT miden movimientos simples se pueden combinar para inferir *el nivel de relajación* -en función de si sus

ii. *Los problemas de ciberseguridad.* La naturaleza técnica de IoT acrecienta el riesgo de ciberamenazas ya que se tratan de "dispositivos con restringida disponibilidad de energía, con ciclos de vida muy largos, situados en lugares muy dispersos y/o accesibles a terceros, y cuyo *firmware* es difícil de actualizar" (Alonso, 2018)[184]. Además hay que tener presente la aparición de las redes 5G que aportarán que otorgarán densidad extrema de dispositivos finales *interconectados* junto con una gran flexibilidad en la provisión y gestión de cada tipo de servicio. Tampoco perdamos de vista que nuestro país haya sido víctima el 80% (además del lugar de origen) de los ataques mundiales en la primera mitad del 2018[185]. Y es que no hay suficientes medidas de seguridad en las plataformas IoT para evitar los ciberataques. La "reidentificación" (o anonimización reversible) es el mayor problema jurídico-técnico. *Paul Ohm*[186] (2010) augura que los avances informáticos cada vez más van a permitir volver a identificar bases de datos supuestamente anónimas[187].

iii. *La falta de capacidad de gestión para llevar a cabo la legitimación jurídica (consentimiento) en el tratamiento de los datos de salud en entornos IoT.* Ya lo decía el GT29, y es que la cadena de suministro en IoT está formada por fabricantes de componentes, capas de transporte, redes y comunicaciones, almacenamiento, consultores, y análisis externos dificulta la gestión de los datos en materia de protección de datos, y en concreto, su legitimación; ¿cómo se deberá recoger el consentimiento en los dispositivos? ¿cómo solicitar el consentimiento de terceros que no son el usuario o cliente del dispositivo (ej. familiares, vecinos, ciudadanos)? A continuación, a modo de ejemplo,

---

movimientos son estables, tembloroso o tensos- al escribir un mensaje de texto o el temblor con el que sostiene el smartphone. Indudablemente el uso y acceso a estos datos podría crear sesgo entre individuos).

[184] Lecuit, J.A. (23 de abril de 2018) . Cifrado, IoT y RGPD: tres desafíos de ciberseguridad en 2018. Real *Instituto El Cano Royal Institute.* Recuperado de http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=%2Felcano%2Felcano_es%2Fzonas_es%2Fari56-2018-alonsolecuit-cifrado-iot-rgpd-tres-desafios-ciberseguridad-2018&

[185] Ver https://www.f5.com/labs/articles/threat-intelligence/the-hunt-for-iot--multi-purpose-attack-thingbots-threaten-intern; ver también https://www.20minutos.es/noticia/3524046/0/espana-pais-castigado-ciberataques-internet-cosas/

[186] Ohm, P. , (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review.* Vol. 57, p. 1701. Recuperado de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006

[187] Por ejemplo, aunque *Fitbit* elimine el nombre, dirección y otra información identificadora del conjunto de datos de un individuo antes compartir la información con otros, la re-identificación sería posible. La razón es clara: cada uno de nosotros tiene un modo de andar único.

señalamos un cuadro comparativo significativo [188] de diferentes dispositivos IoT fitness (Fitbit, Xiaomi, Garmin, etc.) apuntando al tipo de datos que recogen (email de amigos, geolocalización, información de salud reproductiva, etc.):

Data type	Basis	Bellabeat	Fitbit	Garmin	Jawbone	Withings	Xiaomi
Name / DOB / Gender / Heigh / Weight / Email							
Friends' email address(es)		X		X			X
Geolocation	*	X	*	X			X
Phone serial number		X	X	X	X	X	X
IMEI Number	X	X	X	X	X	X	
Wearable MAC address					X		
Steps per time interval and/or heart rate over time	*		*				
Manual activities and/or measurements	X	X					X
Food intake	X	X				X	X
Reproductive health info	X		X	X	X	X	X

Table 3: Sensitive Data Transmissions. For items marked with a "*", we did not directly observe this data being transmitted, as the application encrypted and/or encoded its payloads. However, the user interfaces updated to display the data type following HTTP transmissions.

Tabla 12. Cuadro comparativo de dispositivos IoT de fitness y carecterísticas.

iv. *Maximización de datos y el control excesivo de la actividad humana: "el monitoreo mejorado".* El monitoreo es una condición de la vida moderna (Rule, 1983)[189] donde los dispositivos IoT son "invisibles" e "intrusivos" acarreando riesgos y problemas para las personas.

2.4. Una aproximación a las soluciones posibles.

Algunas de las soluciones que voy a proponer a continuación podrían ser imperfectas -aunque pragmáticas-, y otras están más definidas al estar encuadradas en el propio RGPD:

[188] Open Effect (2016) . Every step you fake. A comparative analysis if fitness tracker privacy and security. Recuperado de https://openeffect.ca/reports/Every_Step_You_Fake.pdf pp. 18
[189] Rule, J. et al. (1983) . Documentary Identification and Mass Surveillance in the United States. *Social Problems* .Vol. 31. No. 2 pp. 222-234. Oxford Universtity Press. Recuperado de https://www.jstor.org/stable/800214?seq=1#page_scan_tab_contents

i. *Brindar a los usuarios un modelo de "autogestión de la privacidad"* (*Daniel Solove*, 2013)[190] y modelo de transparencia de los proveedores. Donde pudieran analizar los riesgos que pueden acarrear el tratamiento de sus datos personales de salud. La nueva normativa da luz al principio de transparencia obligatorio para los proveedores tecnológicos (art. 13 RGPD) "*radical transparencia*" (Hissembaum y Patterson)[191] evitando información opaca e entendible al usuario. Será necesario informar a los usuarios sobre cuestiones concretas[192].

ii. *Medidas de seguridad técnicas y organizativas.* Nos referimos a técnicas de anonimización irreversible que garanticen la protección de los datos personales de categoría especial como son los de salud de obligado cumplimiento. La tecnología blockchain por su naturaleza técnica puede otorgar seguridad y protección ante ataques cibernéticos a la red de IoT donde los datos están alojados en la nube pública.

iii. *Numerosos actores y mayor control en la gestión de la legitimación del tratamiento.* Las medidas anteriores deberán ser incluidas en los contratos de encargo correspondientes entre los actores que intervengan. Los responsables de tratamiento (quienes decidan la finalidad y los medios del tratamiento) podrán exigir a sus encargados de tratamiento (desarrolladores, aseguradoras, universidades u hospitales) la adhesión a códigos de conducta (donde se comprometan los actores a recoger datos agregados no identificados) o la obligatoriedad de que subcontratistas cuenten con un determinado certificado como el ISO/IEC 30141[193]. Por su parte, también blockchain[194] (o sistemas DLT)

---

[190] Solove, D.J. (2013). Introduction: Privacy Self-Management and the Consent Dilemma. Recuperado de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018

[191] Hissembaum, H., Patterson, H. Biosensing in Context: Health Privacy in a Connect World. Recuperado de https://nissenbaum.tech.cornell.edu/papers/Nissenbaum%20H%20Patterson%20H_Biosensing%20in%20Context.pdf

[192] ¿Qué información exacta recoge el dispositivo IoT sobre un usuario? ¿con qué tipo de sensores?¿donde se almacena la información; en el dispositivo, en el smartphone, en los data center del fabricante en la nube, o en todos?: ¿Esa información personal esta encripatada? ; Si la información se almacena en una forma no identificada, ¿el fabricante mantiene la capacidad de volver a identificar la información (ej. anonimizada reversiblemente) o no? ; ¿Puede el usuario portar sus datos?; ¿Puede el usuario ver, editar o eliminar datos del sensor de la servidores del fabricante?; ¿Con qué terceros compartirá los datos el fabricante?

[193] Ver en https://smart-lighting.es/publicacion-la-primera-norma-internacional-iso-internet-las-cosas/ (Ha sido desarrollado por el comité técnico conjunto de la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional: ISO/IEC JTC 1, Tecnología de la información; subcomité SC 41: Internet de las cosas y tecnologías relacionadas).

podrá brindar al usuario un protocolo de inmutabilidad y de compensación monetaria por la cesión o arrendamiento de sus datos a universidades u hospitales).

3. BIG DATA DE LA SALUD

3.1. Introducción

Big data no es una tecnología en sí misma, sino más bien, un planteamiento de trabajo para la obtención de valor y de beneficios como consecuencia del tratamiento de grandes volúmenes generados día a día (CESEDEN)[195]. Así por ejemplo, en el ámbito de la investigación, "las herramientas de análisis que proporciona Big data acortan los tiempos en los procesos de análisis de la información y ofrecen nuevas aproximaciones", y esto "puede conducir a un *contexto de investigación acelerada, de medicina asistida y participativa*" (Martinez, 2017)[196]. Pero el camino es largo; "el gran reto de los datos masivos es la *captación, gestión y tratamiento para agregar valor* a grandes volúmenes de datos poco utilizados o inaccesibles hasta la fecha…" (Cotino, 2017)[197].

3.1.1. Características y tipología de datos en Big Data de Salud.

El Big Data está caracterizado por las conocidas "v": volumen, variedad y velocidad y otras que han aparecido[198]. Ahora bien, conviene adentrarnos en la particularidad del entorno del big data de la salud para conocer su potencial y repercusión en el sector:

---

[194] Recuperado de https://www.coincrispy.com/2017/07/17/bowhead-dispositivo-blockchain/

[195] Grupo de trabajo sobre big data, de la Comisión de investigación de nuevas tecnologías del Centro Superior de Estudios de la Defensa Nacional (Ceseden) (2013). Big Data en los entornos de defensa y seguridad. Documento de investigación 3/2013. Pág. 9.

[196] Martinez, R. (2017) . Big data, investigación en salud y protección de datos personales ¿un falso debate?. *Revista Valenciana de Estudios Autonómicos*, nº 62, pp.237.

[197] Cotino Hueso, L.(2017). Ética de datos, sociedad y ciudadanía. *Dilemata,* año 9, nº 24, 132.

[198] La primera es la más obvia, ya que nos encontramos en continuo cambio de magnitudes (megabytes a terabytes o petabytes). Pero además del volumen, también ha aumentado la tipología de datos, pasando de tratamiento de datos estructurados a desestructurados, semiestructurados; de datos estáticos a dinámicos; provenientes de personas a sensores o máquinas. Y por último, el factor "tiempo" es importante, de aquí que la variable velocidad permita capturar movimiento y proceso de los datos llegando incluso en ocasiones a tiempo real. También se consideran otras nuevas "V"; la variabilidad que implica cambios frecuentes en el significado de los datos o el valor relativo a los ingresos de los datos; o la veracidad relativa a la calidad de los mismos. Vid. Puyol, J. (2014).Una aproximación a Big Data. *Revista de Derecho UNED*, núm. 14, 2014, págs. 471-505.

i. *El big data favorece el progreso médico*. En el ámbito de la prevención de enfermedades, la recolección a largo plazo de datos en diferentes lugares (o poblaciones) permite *identificar factores de riesgo* para ciertas *enfermedades* como por ejemplo, el cáncer[199], la diabetes, el asma o las enfermedades neurodegenerativas.

ii. *Diagnóstico y personalización*[200] *del tratamiento* a través del procesamiento de grandes masas de datos clínicos individuales.

iii. *Prevención de epidemias.* Con amplia información sobre el estado de salud de los individuos en un lugar concreto, se podrá identificar el aumento de la incidencia de enfermedades o conductas de riesgo, y alertar a las autoridades sanitarias. Por ejemplo, el simulador *Gleam*, diseñado para predecir una hipotética propagación de una epidemia concreta, a partir de la explotación de los datos del transporte aéreo[201].

iv. *Fármaco-vigilancia*. Big data ayuda a identificar contraindicaciones indeseables graves y alertar sobre ciertos riesgos. En 2013, la base de datos SNIIRAM permitió estudiar el riesgo de accidente cardiovascular así como el infarto de miocardio en mujeres que utilizaban la píldora anticonceptiva de tercera generación.

Llegados a este punto, resulta imprescindible que diferenciemos entre minería de datos ("big data") y analítica de datos ("*big data analytics")*[202] . Según la ICO[203], la diferencia radica en los siguientes aspectos:

---

[199] La tecnología del big data donde más repercusión está teniendo es en la enfermedad del cáncer y en el tratamiento individualizado gracias al análisis de datos. Los investigadores del CNIO desarrollan *PanDrugs*, una herramienta de prescripción de medicamentos que tiene en cuenta los datos genómicos del paciente. El mayor problema para los especialistas era abordar los diferente tipos de enfermedad. La versión actual de *PanDrugsdb* integra datos procedentes de 24 fuentes primarias y es capaz de generar más de 56000 asociaciones fármaco-diana. Vid en https://www.consalud.es/saludigital/113/nuevo-sistema-basado-en-analisis-de-datos-para-tratamientos-individualizados-contra-el-cancer_51118_102.html

[200] Otro de los ámbitos donde se empieza a aplicar la tecnología del *big data* es para ayudar a la toma de decisiones sobre la inducción al parto (obstetricia). El éxito del procedimiento de inducción está condicionado por variables maternas y fetales que aparecen antes o durante el embarazo. El fracaso de este procedimiento, en muchos casos, puede desencadenar en una intervención por cesárea e, incluso, ocasionar otras complicaciones indeseadas. Para más info: https://www.consalud.es/saludigital/105/el-big-data-llega-a-la-induccion-al-parto_48900_102.html

[201] Los datos indican al menos una vez por semana el número de casos observados de siete enfermedades contagiosas así como de actitudes suicidas y se transmiten a través de una red segura, al Instituto Pierre Louis Epidemiología y Salud Pública de Francia, en colaboración con el Instituto de Vigilancia de la Salud (IVS).

[202] El informe "Big data en salud digital", ya citado, distinguió distinguir en concreto tres tipos principales de análisis. En concreto:

- *Modelos predictivos*: analizan los resultados para evaluar qué probabilidad tiene un individuo de mostrar un comportamiento específico en el futuro con el fin de mejorar la eficacia.
- *Modelos descriptivos*: describen las relaciones entre los datos para poder clasificar a los individuos en grupos.

i. *Uso de algoritmos*. Consiste en una forma de aprendizaje automático donde el sistema "aprende" cuáles son los criterios relevantes del *análisis de datos*.

ii. *Opacidad del procesamiento.* Por lo que es difícil entender los motivos de las decisiones tomadas como resultado de un aprendizaje profundo.

iii. *Uso de todos los datos.* El análisis de big data puede almacenar y analizar cada vez mayor cantidades de datos.

iv. *Reasignación de los datos.* También puede servir para destinar el uso a un propósito diferente de aquel para el cual fue originalmente recogido, con lo que ello conlleva en privacidad.

v. *Nuevos tipos de datos.* Por ejemplo, generados por IoT y la analítica del big data.

Ahora centrémonos en los cinco tipos posibles de datos generados en big data de salud (Soares, 2012)[204];

Web y redes sociales	Contenido web e información obtenida por las RRSS.	Ej. FB, twitter, blogs
Machine-to-machine	M2M utiliza dispositivos como sensores que capturan información y se retransmiten a través de redes alámbricas, inalámbricas o híbridas.	Ej. Temperatura corporal, presión..etc.
Big data transation	Incluye datos de transacciones masivas de centros de at. Telefónica, de banca, atención a clientes.	Ej. Registros de facturación, registros o notas "subjetivas" de llamadas (Call detail record), etc.…
Biométricos	Información biométrica	Ej. Huellas digitales, escaneo de retina, reconocimiento fácil, genética.
Generados por personas[205]	Datos digitales generados por personas.	Ej. Notas de voz, emails, resultados médicos, multas,

- *Modelos de decisión:* describen la relación entre todos los elementos de una decisión, incluidos los resultados de los modelos de predicción, la decisión a tomar y el plan de variables y valores que determinan la propia decisión, con la finalidad de predecir los resultados mediante el *análisis de muchas variables*.

[203] ICO (4 de septiembre de 2017). Big data, artificial intelligence, machine learning and data protection. Recuperado de https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

[204] Soares, S. (3 de junio de 2012). Not your type? Big Data Matchmaker on five data types you need to explore today. *Dataversity*. Vid. http://www.dataversity.net/not-your-type-big-data-matchmaker-on-five-data-types-you-need-to-explore-today/

[205] Algunos ejemplos de Big Data como detector de posibles pautas de comportamiento de salud de una persona o grupo de personas son: (i) *Profiling* que consiste en acumular datos en principio inconexos con el fin de crear un perfil (sanitario o de bienestar) detallado de una persona o de un grupo de personas. El RGPD define en el art. 4.4 la elaboración de perfiles como «toda forma de tratamiento automatizado de

		etc.

Tabla 13. Tipos de datos generados en Big Data.

Llegados a este punto, también, conviene diferenciar entre los diferentes de datos posibles, *per se,* en el contexto de la salud:

Datos estructurados	• Datos clásicos del cliente: • nombre, edad, sexo • Datos clínicos • Puede ser almacenados, consultados, analizados y manipulados
Datos no estructurados	• Recetas de papel • Anotaciones subjetivas/notas manuscritas • Radiografías digitales • Escáneres • Resonancias, tac, imágenes y vídeos digitales. • Datos clínicos
Datos agregados	• Datos médicos generados de una institución médica o por varias • No es fácil debido a intereses empresariales o políticos • Posibilitaría la IA. ej.: Enfoques en la enfermedad, la cartografía de la enfermedad clínica con datos genómicos, la identificación de recomendaciones de atención individualizada
Datos individualizados	• Datos generales del paciente, enfermedad, ubicación, tratamiento, HCE, síntomas.

Tabla 14. Tipos de datos generados en el contexto de salud.

3.1.2. Aplicabilidad real del Big Data de Salud.

datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física»; (ii) *Personalizing* que consiste en valorar diferentes características de una persona como su estado de salud; (iii) *Tracking* que consiste en seguir a una persona en base al rastro que deja, por ejemplo en Internet, por medio de la información de su salud que deja en las redes sociales.

En 2017, desde el Parlamento Europeo se impulsa a la Comisión Europea acerca de la creación de un grupo de trabajo[206] (*Million European Genomes Alliance*) paneuropeo sobre datos sanitarios para la realización de un *banco de millones de genomas humanos*[207].

Por su parte, en España; ya hay iniciativas en marcha como las siguientes;

i. *El Instituto de Investigación Sanitaria del Hospital Clínico de Valencia*, *Incliva*, participa en un proyecto de big data denominado *"Big Medilytics"* que supone la mayor iniciativa financiada por la UE para transformar el sector de la salud mediante el uso de *big data*. El *Incliva* es uno de los socios principales de este consorcio europeo, liderado por *Philips*, en el que participan 35 entidades de diferentes países. El Instituto del Clínico juega un papel esencial en el proyecto, ya que, junto a la participación científica, es responsable de la comunicación social y de establecer las normas que regulan la *protección de datos y la privacidad de la información* en colaboración con la Universitat de València-Estudi General. El análisis procederá de pacientes, proveedores de atención médica, aseguradoras de salud y proveedores de tecnología médica.

ii. *El Instituto Tecnológico de Informática (ITI), la Universidad Politécnica de Madrid, el Servicio Madrileño de Salud y la empresa Atos Spain S.A.*

iii. *El Instituto Carlos III*, pionero por financiar proyectos de *Big Data Analytics* Sanitario, ha puesto en marcha proyecto *Predictive-Ictus*[208] para ayudar en la toma de decisiones en el ámbito predictivo y preventivo. Será un sistema de información basado en la evidencia y en la experiencia generada a partir de los datos almacenados (anonimizados) en los registros de Diraya[209] y otros datos, enfocado a la prevención de la aparición del ictus en la población de riesgo.

---

[206] Recuperado de: https://www.eureporter.co/health/2017/05/05/eapm-meps-urge-commission-to-ramp-up-big-data-initiatives-in-health-care/

[207] Al otro lado del océano, en EEUU, el grupo de trabajo de expertos de la Universidad de Standford, propone un mecanismo que vuelve *anónimos el 99,7% de los datos genéticos* de los participantes en los estudios. En vez de compartir los genomas secuenciados completos, el método identifica las combinaciones genéticas específicas de cada persona y las coincidencias con otros genomas. De esta manera minimiza la cantidad de información que se necesita para estudiar la enfermedad, pero el riesgo a la intrusión a la privacidad no es cero.

[208] Ver en http:// www.nasonline.org/programs/sackler-colloquia/ completed_colloquia/Big-data.html

[209] El consorcio de empresas lo forman: Indra y Drimay en Andalucía, y Xtrem y Casaverde Hospitales en Extremadura.

iv. *Siemens* ha creado una herramienta llamada *Teamplay*, contando con la colaboración de 153 Instituciones conectadas a la red con más de 2.500 equipos activos compartiendo datos y convirtiéndolos en información, y 300.000 estudios.

v. *Mendelian y Savana* están revolucionando el escenario de la gestión de los macrodatos. *Savana* como *machine learning* "digiere" información simplificada y la pone a disposición de los profesionales sanitarios, basándose en algoritmos mejora el diagnóstico de enfermedades y posibilita la digitalización de historias clínicas (utilizando la anonimización) . Por otro lado, *Mendelian* es una web gratuita para profesionales, pacientes e instituciones que permite la gestión de millones datos de las enfermedades raras.

Imagen 26. Ejemplos de plataformas de machine learning en salud. Fuente: Mendenian y Savana

¿Qué ventajas y desafíos generales trae el Big Data de salud?

Los efectos (positivos) del despliegue del big data en salud se materializarán en la "medicina de las 4p: personalizada, predictiva, preventiva, participativa y poblacional" (Muyol, 2016)" . Es decir, en la sostenibilidad de la salud reduciendo el coste sanitario, una mayor calidad en la atención sanitaria, mejor adecuación de los fármacos y la propulsión de la conocida. Esta tecnología permite un aumento de control asistencial[210] médico y mejora la comunicación con el ciudadano.

Respecto a los desafíos generales de esta tecnología conviene resaltar los señalados por la Unión Internacional de Telecomunicaciones[211]. Me gustaría destacar principalmente los siguientes; por un lado, *la heterogeneidad de los datos y los datos incompletos:* los datos procesados a partir de Big Data pueden pasar por alto algunos atributos o introducir "ruido estadístico" en la transmisión de los mismos datos. Incluso

[210] En Reino Unido, el proyecto *Routes to Diagnosis de la Public Health England* (PHE) en 2009 sirvió para averiguar cómo fueron las personas diagnosticadas de cáncer. Se llegaron a analizar 118 millones de registros en 2 millones de pacientes de varias fuentes de datos. Se descubrió el 25% de los casos detectados eran descubiertos en situación de emergencia médica, de esta manera, en 2013 pudieron reducirlo al 20% gracias a iniciativas públicas como *PHE Be Clear on Cancer.* Para más información: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

[211] Recomendación UIT-T Y . 3600 (2015) Grandes volúmenes de datos-requisitos y capacidades basados en la computación en la Une. Recuperado

después de realizar una limpieza de datos y una corrección exhaustiva, es probable que permanezcan errores. Este reto puede ser en parte solventado durante el análisis de datos. Y por otro lado; *la privacidad:* los datos acerca de los individuos, tales como la información demográfica, las actividades de Internet, los patrones de comportamiento, las interacciones sociales o el uso de energía están siendo recogidos y analizados para diferentes propósitos. A continuación, profundizaremos algo más sobre ello y más cuestiones.

3.2. Riesgos y la protección de datos.

El profesor Martínez[212] señala que "se ha defendido la necesidad de desarrollar un enfoque cualitativo que sea capaz de *poner en valor tanto los riesgos como los beneficios* derivados del tratamiento de información personal, e integrar la interpretación jurídica en el marco del preciso *contexto social, económico y tecnológico* en el que se desarrollan los tratamientos". Este autor hace referencia al Convenio 108/1981[213] y a la memoria explicativa, por el que se señala *que "los datos sensibles pueden ser lesivos por sí mismos"*. No obstante, como bien indica, no deberíamos adoptar una "postura apriorística", sino más bien todo lo contrario, vistas las ventajas que aportan las tecnologías en el desarrollo de la sociedad y a la mejora de la calidad de vida de las personas.

Según el profesor Cotino[214], una de las premisas jurídicas es determinar y en su caso *diferenciar el tratamiento jurídico de la actividad de big data* si se realiza por poderes públicos o por el sector privado, teniendo en cuenta también, la concurrencia de

[212] Martinez, R. (2017). Big data, investigación en salud y protección de datos personales ¿un falso debate?. *Revista Valenciana de Estudios Autonómicos*, nº 62, pp.239. En III Congreso Internacional sobre Protección de Datos de la Cátedra Google de Privacidad. Martínez, R. «Protección de datos y desarrollo tecnológico en un mundo global», en el BLOG LOPD y Seguridad. Recuperado de http://lopdyseguridad.es/proteccion-de-datos-y-desarrollo-tecnologico-en-un-mundo-global/

[213] BOE, núm. 274, de 15 de noviembre de 1985. Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981.Recuperado de https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447. (La memoria explicativa del Convenio señala: "Si bien el riesgo de que el procesamiento de datos sea dañino para las personas generalmente *no depende del contenido de los datos*, sino del contexto en el que se encuentran utilizado, existen casos excepcionales en los que el procesamiento de determinadas categorías de datos *es en sí mismo probable que conduzca a usurpaciones de los derechos e intereses individuales…")*

[214] idem

posibles obligaciones de transparencia y puesta a disposición de los datos abiertos para su reutilización[215].

Como posibles retos o desafíos específicos a superar en el ámbito de los proyectos de *big data y eHealth*, podemos enumerar los siguientes:

i. El reto de la discriminación.

En el considerando P de la Resolución del Parlamento Europeo sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI))[216] establece que;

> "la *proliferación del tratamiento y la analítica de datos*, la infinidad de agentes que intervienen en la recopilación, la conservación, el tratamiento y el intercambio de datos, así como la combinación de grandes conjuntos de datos que contienen datos personales y no personales procedentes de distintas fuentes, si bien brindan oportunidades significativas, todos ellos han generado una *gran*

[215] En un estudio de *Wellcome Trust (*Ver en https://wellcome.ac.uk/sites/default/files/wtp053205_0.pdf), los encuestados conciben el tratamiento de datos de salud como positivo si se realiza en el contexto de la NHS (Sistema de Salud Nacional inglés). Los ejemplos más claramente *beneficiosos* de recopilación y uso de datos de salud entre los entrevistados fueron los datos que servían para vigilar la enfermedad de la varicela, los datos e informes de médicos de sarampión de la junta de salud o los datos de auditoría , como por ejemplo, comparar tasas de mortalidad hospitalaria, los datos de salud sexual (encuesta nacional - NATSAL) y los datos de salud mental (biobanco del Reino Unido - estudio a largo plazo). Los encuestados los concebían como beneficioso potencialmente para la sociedad en los campos de investigación, prevención de enfermedades, planificación de servicios, prevención del delito, pero la situación cambiaba cuando se trataban de compañías de seguros, empleadores o fabricantes de medicamentos. Los datos de salud de la población se consideran anónimos, de beneficio para todos y tranquilizadores para ser recolectados por el bien común, especialmente a largo plazo. Sin embargo, la posibilidad de identificar individualmente sí que preocupa, sobre todo si esos datos acaban en las "manos equivocadas". Con la *investigación genética y el procesamiento de datos de salud en enfermedades raras* surgieron interrogantes sobre todo relacionado con que los medios pudieran sacarlo a luz y provocar estigmación o exclusión individual .

[216] Parlamento Europeo (20 de febrero de 2017). Propuesta de Resolución sobre las implicaciones de los macrodatos en los derechos fundamentales; privacidad, protección de de datos, discriminación, seguridad y aplicación de la ley. Recuperado de http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0044+0+DOC+XML+V0//ES

inseguridad tanto para los ciudadanos como para los *sectores público y privado* en lo que se refiere a los requisitos específicos para el cumplimiento de la legislación vigente en la Unión en materia de protección de datos".

ii. Finalidades (in)compatibles y legitimación.

En primer lugar, hablemos de las finalidades de tratamiento y de la aplicación del principio de limitación de finalidad (Art. 5.1.b RGPD) en los proyectos de big data de salud.

Esta tecnología por su propia naturaleza puede derivar a situaciones en las que la finalidad inicial del tratamiento de información personal (o el dato en cuestión) resulte "difuminada" una vez que el dato es explotado (ISMS Forum y AEPD)[217]. Continuando con el ámbito de la salud, el Comité Internacional de Bioética[218] predijo que en el caso de biobancos donde se utiliza dicha tecnología, el posible uso secundario de datos en el futuro no puede predecirse. Y es que no siempre se conoce desde el inicio el alcance del proyecto, por todo ello, será necesario hacer referencia a que los datos personales no podrán usarse para *finalidades incompatibles* con aquellas para las que los datos hubieran sido recogidos. Lo que no significa que no puedan utilizarse para finalidades diferentes para las que se recogieron, si no que éstas no deben ser incompatibles.

En materia de *investigación científica*, el legislador comunitario se pronuncia flexible[219] para tratamientos posteriores considerando ciertos casos como no incompatibles con los fines iniciales, entendiendo posiblemente la dificultad de la que hablamos. El art. 5.1.b RGPD señala que los datos personales;

> "...*no serán tratados ulteriormente de manera incompatible con dichos fines*; de acuerdo con el artículo 89, apartado 1[220], el tratamiento ulterior de los datos personales con fines de archivo en

[217] Vid. http://www.ismsforum.es/ficheros/descargas/codigo-buenas-practicas-para-proteccion-de-data.pdf
[218] Vid. http://unesdoc.unesco.org/images/0024/002487/248724e.pdf pp.12
[219] Hay que tener en cuenta que intentar equilibrar la privacidad y el interés del público (más amplio) no es tarea fácil porque puede entrar en conflicto. El ICB establece que no son opuestos sino que están relacionados:" hay intereses privados en el logro objetivos comunes y un interés público en la protección de la privacidad que fomenta cooperación. Esta compleja relación lleva a una necesidad de conciliar la articulación de lo privado dentro del público y lo público en lo privado".
[220] Señala que; "el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las *garantías adecuadas*, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de *medidas técnicas y organizativas*, en particular para garantizar el respeto del *principio de minimización* de los datos personales. Tales medidas podrán incluir *la seudonimización*, siempre que de esa forma puedan

interés público fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»)"

Pongamos un caso real. En el estudio, ya citado a lo largo del trabajo, *Wellcome Trust*, para los encuestados resultó una cuestión controvertida y no esperada que el gobierno "husmeara" los hábitos de compra de los pacientes a través de los datos de las tarjetas *anónimas* de fidelización, para medir la salud pública e investigar si eran adecuados en relación con los estados de salud de los mismos.

En todo caso, el análisis de *no incompatibilidad* es esencial en los proyectos de big data, dado que la mayoría de las ocasiones, se basan sus analíticas en el tratamiento posterior con finalidades adicionales a la finalidad original. El Grupo de Trabajo del Artículo 29 ha analizado este aspecto en su Dictamen (WP 203)[221], estableciendo los siguientes criterios para saber si los usos posteriores de los datos personales son compatibles o no;

- Debe existir una *relación* entre la finalidad original y la finalidad o finalidades ulteriores.
- El tratamiento ulterior debe encontrarse dentro de las *expectativas razonables* del interesado.
- Debe tenerse en cuenta la *naturaleza de los datos* objeto de tratamiento y la sensibilidad de los mismos. Los datos de salud son de categoría especial.
- Debe considerarse el *impacto* que este tratamiento va a tener en los interesados.
- Deben considerarse las *medidas de protección* que el responsable del tratamiento establece, en particular las medidas técnicas y organizativas: encriptación, pseudonimización, separación funcional, transparencia, oposición al tratamiento". Según el WP 203 para identificar qué salvaguardas son necesarias, puede ser útil hacer una distinción entre dos escenarios diferentes.

En segundo lugar, y tenemos que centrarnos en la legitimación por consentimiento (9.2. a. RGPD), preguntándonos ; ¿cómo se podría otorgar un consentimiento (informático) informado válido, por ejemplo, en proyectos de big data de salud? [222]

---

alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior *que no permita o ya no permita la identificación de los interesados*, esos fines se alcanzarán de ese modo".

[221] Vid. GT29, Opinion 03/2013 on purpose limitation https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp203_en.pdf.

[222] Ya en la *Declaración Universal sobre Bioética y Derechos humanos* (UDBHR), en el artículo 6 se establece que cualquier intervención médica preventiva, diagnóstica y terapéutica también solo debe llevarse a cabo *"con el previo, libre, expreso e informado consentimiento de la persona interesada"* (UNESCO, 2005). Además, ya el *Código de Nuremberg se* centraba en el consentimiento y concibe la participación en la investigación como una actividad voluntaria al igual que la De*claración de Helsinki* también consagra el consentimiento como garantía principal.

El Comité Internacional de Bioética da una posible respuesta: un nuevo modelo de consentimiento más apropiado que permita un amplio tratamiento de datos respetando al mismo tiempo la autonomía del individuo; denominado *"consentimiento amplio"*.

Otro enfoque tendría que ver con el *"consentimiento de exclusión"* según el cual los datos de salud se pueden utilizar para fines de investigación a menos que un individuo se excluya afirmativamente.

Pero además, también se podría hablar del *"consentimiento dinámico"* con base en el consentimiento inicial el cual implica una *actualización* sobre el uso de datos de *forma continua* para que el individuo pueda optar por usos específicos (se me ocurre, a través de interfaces entre dispositivos y un programa). Este consentimiento requerirá (inevitablemente) de la participación de los poderes públicos para garantizar los derechos individuales y dar información y educación al respecto sobre todo en países desarrollados. Investigador y paciente estarían conectados y podría funcionar como una empresa prácticamente (Consejo Nuffield, 2015)[223] donde el equilibrio de poder se intenta instaurar.

Ahora bien, ¿podríamos aplicar estos modelos de consentimiento a los usuarios de eHealth donde haya datos masivos y analítica con tratamientos de datos de salud con finalidades diferentes a la de la investigación científica (Art. 5.1.b; 89.1 RGPD) sirviéndonos de la propia tecnología a través de interfaces o APIS o incluso del protocolo blockchain y/o sistemas DLT? En mi humilde opinión, no entiendo porque no podría ser posible siempre que permite la "autogestión de la privacidad" al usuario.

iii. Falta de transparencia y desequilibrio en la información.

Como hemos establecido el consentimiento en eHealth puede suponer un gran desafío ya que la información se escribe en caracteres pequeños en los Smartphone, donde el individuo no puede consultar y acaba aceptando de manera inmediata sin haber obtenido la información suficiente para tomar una decisión adecuada. El SEPD[224] consideró dos desafíos interconectados: la falta de transparencia de las organizaciones

[223] Nuffield Council on Bioethics (2015). *La recopilación, vinculación y uso de datos en biomedicina investigación y cuidado de la salud: cuestiones éticas*. Recuperado de http://nuffieldbioethics.org/wp-content/uploads/Biological_and_health_data_web.pdf

[224] EDPS. Opinion 7/2015 Meeting the challenges of big data https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf

respecto al tratamiento que realizan a la información y el desequilibrio en la información entre las personas y las organizaciones que tratan sus datos personales.

En primer lugar, preguntémonos; ¿cómo se puede garantizar dicha *transparencia*? Teniendo en cuenta lo que aporta el Dictamen WP203[225] y otras fuentes seremos capaces de dar algunas pinceladas a modo de respuesta:

a. Los interesados deberían tener acceso[226] a sus "perfiles", así como a la lógica de la toma de decisiones algorítmicas. Sería importante que los individuos pudieran corregir o actualizar sus perfiles si así lo desean, de esta manera también se podría ayudar a minimizar prácticas discriminatorias.

b. La gobernanza[227] tiene que compensar la pérdida de control asegurando que se respetan todas las dimensiones de la autonomía (ICB, 2015). También se debería revelar la fuente de los datos que condujeron a la creación del perfil.

c. Lo ideal además sería que se pudiera estar ante una información del tratamiento de datos en formato portátil y de fácil lectura (el GT29 lo denomina *"portable, user-friendly and machine-readable"*) de esta manera se podría compensar la desigualdad económica entre organizaciones y titulares de datos, de forma que se les empodere.

En segundo lugar, hablemos de equilibrio de poder en la información y autonomía individual. El Comité internacional de Bioética de la Unesco (IBC) en su informe sobre Big Data y e-Health[228] trata la cuestión de la *falta de autonomía individual,* estableciendo que la autonomía de un individuo en términos de ejercicio de su autodeterminación incluye varias dimensiones (Mertz et al., 2016)[229]; (i) la competencia del individuo interesado para acceder, comprender, evaluar y para aplicar información relevante; (ii) la información debe estar disponible que sea relevante y comprensible para el pregunta en juego; (iii) tiene que haber una opción entre diferentes

[225] Ver info: https://cnpd.public.lu/dam-assets/fr/publications/.../wp203_en.pdf

[226] Ver iniciativas como *'midata'* en el Reino Unido, que se basan en el principio clave de que los datos deben ser publicados de vuelta a los consumidores. La idea clave es que los consumidores también deberían beneficiarse del big data al tener acceso a su propia información para permitirles tomar mejores decisiones. Ver: https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment

[227] Puede ser de nuestro interés la guía de la OCDE (2017) llamada *Recomendación sobre Gobernabilidad de Datos de Salud* donde se destaca la importancia de complementar la protección jurídica de los datos a través de la educación y la sensibilización, el desarrollo y la promoción de medidas técnicas.

[228] *supra cit.*

[229] Mertz M., Jannes, M., Schlomann, A., Manderscheid, E., Rietz, C. y Woopen, C. 2016. *Digitale Selbstbestimmung* . Centro de Ética, Derechos, Economía y Social de Colonia Ciencias de la Salud. DOI 10.8716 / ceres / 00001.

opciones, ya sea la de hacer; (iv) o abstenerse de hacer algo o el uno entre hacer cosas diferentes; (v) los valores del individuo, sus preferencias y actitudes se toman en cuenta al decidir y actuar; (vi) se otorga voluntariedad para que el individuo pueda decidir y actuar sin interna o coerción externa; (vii) la formación de la voluntad se refiere a la capacidad del individuo para elegir un objetivo y medios apropiados para alcanzarlo; (viii) la acción puede significar un hacer consciente o abstenerse.

d. Anonimización reversible como problema.

Si los datos personales pueden ser completamente anonimizados[230], ya no son personales datos y por tanto no se aplicará la legislación de protección de datos.
Consiste en disociar los datos de manera tal que no se no permita la identificación de un afectado o interesado sirve paras eludir riesgos y la aplicación de la normativa. La anonimización exige que*: (i)* no pueda ser establecido vínculo alguno entre el dato y su titular sin un esfuerzo desproporcionado; (ii) sea irreversible; (iii) en la práctica sea equivalente a un borrado permanente (Martinez, 2017). Para el GT29, en la anonimización siempre existen riesgos como la posibilidad de reidentificar mediante inferencias, o por vinculación o link con otros paquetes de datos personales. Dicho esto, se requerirá de una anonimización que no sea reversible para evitar que los datos sean de nuevo identificados con personas. Según Jesús Rubí (2015)[231], ante este escenario se podrían emplear mecanismos como los *contratos de compromisos de información* o de *penalización ante incumplimiento* -no sólo económicos-; códigos-tipo de farmaindustria y certificaciones, u otros que se determinen una vez analizada el tipo de información médica, la tecnología o los tipos de centros de salud.

e. La cuarta "v" de veracidad y su desafío.

[230] Existe bastante discusión al respecto acerca de si la anonimización hace ineficaces los tratamiento de datos. El problema no es tanto si se puede eliminar el riesgo y producir la reidentificación por completo sino si se puede mitigar el riesgo hasta que sea totalmente improbable. Esto no hace que la anonimización sea imposible, por tanto. Según la ICO, "las organizaciones que utilizan datos anonimizados deben ser capaces de demostrar que han evaluado robustamente el riesgo de reidentificación, y han adoptado soluciones proporcionales al riesgo" (AEPD ISMS, 2017) .

[231] Ver https://www.youtube.com/watch?v=716SW-TS71w . *Archivo y flujo de datos. Universidad Deusto e Instituto*

La posible inexactitud e imprecisión en la colección y clasificación de los datos puede unida a la cantidad de datos y de diferentes fuentes, la desordenada gestión y los diferentes contextos son otro de los retos al que se enfrenta esta tecnología. Piénsese por ejemplo en registros que no son completos, en clasificaciones incorrectas o información falsa[232].

3.3. Una aproximación a las posibles soluciones

i. Ética de datos y responsabilidad activa.

Partimos de la idea de que la ética e integridad son fundamentales para cualquier proyecto vinculado a Big data. En este sentido y orientada esta ética de datos al principio de accountability, el GT29[233] hace hincapié en algunas de forma expresa. También me resulta de interés destacar la nueva figura de la *"responsabilidad algorítmica"*[234], consistente en comprobar que los algoritmos utilizados y desarrollados

[232] Según un estudio, los individuos dan deliberadamente a las organizaciones datos falsos sobre ellas mismas para proteger de alguna manera su privacidad. En el marco del *Future Trends Forum* se pudieron plantearon concretamente tres problemas: (i) la limpieza de los datos basura; (ii) la comprensión lectora y su aplicación práctica; (iii) tiene que ver con la ética y la responsabilidad. Ver en https://www.marketingweek.com/2015/07/08/consumers-are-dirtying-databases-with-false-details/

[233] Como por ejemplo; el establecimiento de procedimientos internos previos a la creación de nuevas operaciones de tratamiento de datos personales (revisión interna, evaluación, etc.); el establecimiento de políticas escritas y vinculantes de protección de datos que se tengan en cuenta y se valoren en nuevas operaciones de tratamiento de datos (p.ej., cumplimiento de los criterios de calidad de datos, notificación, principios de seguridad, acceso, etc.) que deben ponerse a disposición de las personas interesadas; la cartografía de procedimientos que garanticen la identificación correcta de todas las operaciones de tratamiento de datos y el mantenimiento de un inventario de las mismas; el nombramiento de un delegado de protección de datos; la oferta adecuada de formación en protección de datos a los miembros del personal; esto debe incluir a los responsables de los procesos de datos personales (como los directores de recursos humanos), pero también a los administradores de tecnologías de la información, desarrolladores en general, y directores de unidades comerciales; el establecimiento de un mecanismo interno de resolución de quejas de los interesados. En este ámbito puede jugar un papel destacado el DPO; el establecimiento de procedimientos internos de gestión y notificación eficaces de fallos de seguridad (violaciones de seguridad); la realización de evaluaciones de impacto sobre la privacidad en circunstancias específicas; la aplicación y supervisión de procedimientos de verificación que garanticen que las medidas no sean sólo nominales, sino que se apliquen y funcionen en la práctica (auditorías internas o externas).

[234] Taneja, H. (8 de septiembre de 2016). The need for algorithmic accountability. *TechCrunch.* Recuperado de https://techcrunch.com/2016/09/08/the-need-for-algorithmic-accountability/

por el sistema de machine learning no están haciendo actos discriminatorios, erróneos o injustificados.

ii. Privacidad desde el diseño. Blockchain/DLT.

En la práctica, implica tener en consideración la privacidad y el cumplimiento de las normativas de protección de datos desde la fase inicial del proyecto con el objetivo de que el proyecto se diseñe e incluso ajuste y desarrolle teniendo en consideración dichos requerimientos, de tal manera que la privacidad se integre en las nuevas tecnologías y prácticas empresariales directamente, desde el principio, como un componente esencial de la protección de la privacidad (ISMS AEPD, 2017)[235]. Se puede ver con el art. 25 y el considerando 78 del RGPD que el legislador piensa en medidas técnicas de minimización, pseudonimización, anonimización, etc. Ahora bien, ¿podríamos buscar encaje a *Blockchain/DLT*[236] como medida técnica y de organización para conseguir privacidad desde el momento cero del proyecto big data? A través de ella se podría otorgar al individuo un sistema de "autogestión de la privacidad" donde incluso podría monetizar sus datos en el momento que los "alquila" a entidades que encuentran un provecho económico en ello.

iii. Gobernanza de datos y anonimización irreversible.

Para que se pueda garantizar una cultura de privacidad acorde a las nuevas exigencias, el papel del *data gobernance* de las organizaciones será imprescindible. Los sistemas de control, monitorización y *anonimización*[237] junto a políticas preventivas,

---

[235] D'Acquisito, Giuseppe et al. (diciembre 2015) Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics. *ENISA*. Recuperado de https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/big-dataprotection

[236] Vid. https://bitcoinist.com/big-data-blockchain/

[237] "La anonimizaciónpuede utilizarse cuando los datos se comparten externamente o dentro una organización. Por ejemplo, una organización puede contener un conjunto de datos contener datos personales en un almacén de datos, y producir un versión anonimizada de ella para ser utilizada para análisis en un área separada" Vid. Anonymisation Network website http://ukanon.net/

"Si permanece como datos personales dependerá de si el "claves" de anonimización y otros datos relevantes que permiten la identificación es mantenida por la organización. Incluso si los datos permanecen datos personales, esta sigue siendo una salvaguarda relevante a considerar para que el procesamiento puede cumplir con los principios de protección de datos. La Red de Investigación de Datos Administrativos es un ejemplo de cómo se desidentificó los datos pueden ser utilizados para investigación Los ADRC no tienen identificadores personales con el datos; en su lugar, los identificadores personales se envían a terceros de confianza fiestas." Vid. Administrative Data Research Network https://adrn.ac.uk/protecting-privacy/

proactivas y mitigadoras de riesgos internas que cubran lo que no está cubierto en los marcos legales serán las herramientas a utilizar por el delegado de privacidad o el comité multidisciplinar que trabaje para este fin. Adquirirán especial protagonismo la gestión del consentimiento y la transparencia de cara del e-paciente[238].

Pongamos un ejemplo de datos anonimizados en Big Data Analytics. En la herramienta de Telefónica ("*smart steps"*)[239] los datos identificativos de los clientes se eliminan antes de ser analizados y los datos anonimizados se agregan para obtener información sobre la población como un todo y combinado con datos de investigación de mercado de otros fuentes.

3.4. Fases del proyecto big data aplicado al cuidado de la salud.

Me parece que podría ser interesante aplicar la tabla que ha elaborado acertadamente el profesor Martínez (2017, 249)[240] (quien se sirvió de la clasificación de las cuatro fases indicadas en el *Informe de Big Data en Salud digital de Vodafone*, 22-4)[241]:

Fase	*Objeto*	*Principio Jurídico*
Preguntas iniciales	Definir las preguntas que dan lugar al objeto del proyecto	Finalidad, proporcionalidad
Creación del modelo	• Definir objetivos definitivos así como la estrategia para alcanzarlos. • Integrar un proceso completo para poder capturar, consolidar, gestionar y proteger la información necesaria.	Finalidad, proporcionalidad, políticas de seguridad y perfiles de los usuarios.

[238] Como establece la AEPD ISMS (2017): "El usuario debe conocer en todo momento, de forma sencilla, qué información personal se utiliza y para qué se utiliza, así como permitir que pueda o no dar su consentimiento, e incluso posteriormente oponerse al tratamiento". Además, "se deberán implantar los sistemas de control de acceso, monitorización y anonimización necesarios, para que el análisis se adecúe a las normativas de protección de datos, unido a la creación de políticas preventivas y mitigadoras de riesgos que puedan cubrir aspectos no contemplados por esos mismos marcos legales.

[239] Vid. http://dynamicinsights.telefonica.com/488/smart-steps

[240] *Supra cit.* pp. 249.

[241] Fundación Vodafone España y Red. Es. *Big data en salud digital.* Informe de resultados. Recuperado de http://www.fundacionvodafone.es/sites/default/files/informe_big_data_en_salud_digital.pdf pp.22

	• Identificarse los recursos humanos disponibles para llevar a cabo la implementación del modelo.	
Elección tecnológica	• Escoger soluciones de hardware y software adecuadas.	Seguridad (ISO 17799, Cobit, ITIL, ISO 27000) , transferencias internacionales de datos, encargado del tratamiento
Implementación del modelo	• Obtención y almacenamiento de los datos [242](SQL o NOSQL). • Procesamiento. • Visualización.	Legitimación para el tratamiento, consentimiento, calidad de los datos, proporcionalidad, finalidad, veracidad.

Tabla 15. Ejemplo de fases en el proyecto big data de salud.

4. INTELIGENCIA ARTIFICIAL Y MACHINE LEARNING DE LA SALUD

El Big Data está relacionado y conectado con la Inteligencia Artificial y gracias a ello, ésta última es capaz de aprender, resolver problemas y tomar decisiones. En esta línea, el Parlamento Europeo recuerda que con los *macrodatos* en algunos casos se capacitan de "dispositivos de inteligencia artificial "como redes neuronales y modelos estadísticos con el fin de predecir algunos acontecimientos y comportamientos (Considerando b, 2017)[243]. La medicina ha experimentado una evolución; en primer lugar era "intuitiva" -basada en síntomas-, después se convirtió en basada en "evidencias" -por medio de patrones- y en último lugar, se llamó de "precisión" -basada en algoritmos-. He aquí, la inteligencia artificial en salud[244].

[242] Gómez Pinzón, J.C. (2017). *Implementación de proyectos de Big Data*. (Informe final monográfico, Universidad Libre de Colombia). Págs. 8-11. Recuperado de https://repository.unilibre.edu.co/bitstream/handle/10901/11214/Implementacion%20de%20proyectosde%20Big%20Data.pdf?sequence=1&isAllowed=y

[243] *Supra. Cit.*

[244] Ahora bien, como establece profesionales como el Dr. *Julio Mayol*, las tecnologías innovadoras deberán trabajar más en ciertas cuestiones para que el negocio IA salud se consolide; (i) *Desarrollo en imagen.* Deberán existir técnicas híbridas que fusionen imágenes hasta que el cuerpo humano sea anatómica y molecularmente transparente, codificable e interpretable mediante sistemas de inteligencia artificial; (ii) *Desarrollo en biología y la sociología.* Deberán ayudar a entender mejor los factores que influyen en los estados de salud y de enfermedad con ayuda de la bioinformática; (iii) *Desarrollo en sensores y IoT.* Deberán convertir el diagnóstico y el tratamiento en transparente no invasivo ni intrusivo

Y es que cada año se publican 160.000 artículos científicos relacionados con el cáncer**;** sólo en Estados Unidos, todos los meses, arrancan más de un centenar de ensayos clínicos; y un médico general, para estar al día de las novedades de su campo, tendría que revisar diariamente unas 8.000 investigaciones[245]. Según la revista Forbes, para el año 2025, los sistemas de IA se habrán implementado en el 90% de EEUU y en el 60% de los hospitales y aseguradoras del mundo [246] y esta realidad futura ya ha sido contemplada incluso por las Instituciones Comunitarias.

4.1. Introducción.

4.1.1. Concepto de Inteligencia Artificial.

La definición de *Wikipedia*[247] es que la inteligencia artificial (IA) es "inteligencia exhibida por las máquinas". En informática, una máquina "inteligente" ideal es un agente racional flexible que percibe su entorno y toma medidas que maximizan sus posibilidades de éxito en algún objetivo. Podríamos decir que, las principales características de AI son; por un lado, la recopilación de grandes cantidades de información del entorno que los rodea y; por otro lado, la capacidad de tomar decisiones o acciones autónomas para un fin determinado.

4.1.2. Historia y concepto de algoritmo.

Los babilonios emplearon los algoritmos para organizar leyes, los doctores se han respaldado en algoritmos para asignar diagnósticos[248]; e innumerables personas de todos

---

para el paciente. Se generarán datos y patrones de señal de manera remota con geolocalización, lo que facilitará la monitorización, e incluso el diagnóstico, en tiempo real para pacientes con enfermedades crónicas y el control del estado de salud; (iv) *Desarrollo en biométrica.* Permitirá las interacciones más naturales entre humano y máquina en imagen, reconocimiento de tacto, lenguaje y lenguaje corporal; (v) *Desarrollo en analítica de textos y procesamiento de lenguaje natural*. Será necesario para el análisis de notas clínicas. Son cuestiones importantes ya que hacen que IA interactué de manera estrecha con el resto de las tecnologías que tratamos en este trabajo. En verdad, todas las tecnologías se necesitan entre sí.

[245] Jiménez, J. (2016). Ya no se puede practica bien la medicina sin una inteligencia artificial al lado. *Xataca*. Recuperado de https://www.xataka.com/medicina-y-salud/ha-llegado-el-momento-en-que-no-podremos-practicar-la-medicina-sin-una-inteligencia-artificial-al-lado

[246] Rouse, M. (2015). IoMT or healthcare IoT. *IoT Agenda.* Recuperado de http://internetofthingsagenda.techtarget.com/definition/IoMT-Internet-of-Medical-Things

[247] Ver en línea: https://en.wikipedia.org/wiki/Artificial_intelligence

[248] Gayo, M. (9 de enero de 2019). La inteligencia artificial ayuda a identificar síndormes genéticos raros. *ABC Enfermedades*. Recuperado de https://www.abc.es/salud/enfermedades/abci-inteligencia-artificial-ayuda-identificar-sindromes-geneticos-raros-201901071700_noticia.html

los rincones del planeta han intentado predecir el futuro con ellos (Chabert, 1999)[249][250]. El nombre álgebra viene directo del nombre al-Jabr del título en el libro. Como los escolares diseminaron el trabajo de Al-Khwarizmi en Latín durante el Medioevo, la traducción de su nombre-"algorism"-fue utilizada para describir cualquier método de cálculo sistemático o automático (Chabert, 1999). En el S. XVII, Leibniz creía que el futuro de los objetos podría ser predicho al examinar sus conexiones (Russel, 2008)[251] y esto se ha reflejado en la era contemporánea e incluso en Wall Street. Y él antes que nadie concibió algo cercano a la inteligencia artificial, estipulando que el pensamiento cognitivo y la lógica podrían ser reducidos a una serie de expresiones binarias (operaciones mecánicas por máquinas diseñadas por él). Cuanto más complicado el pensamiento, más simples deberían ser los conceptos necesarios para describirlo (Steiner, 2012). Fue Leibn quien desarrolló elegantes notas para las funciones integrales y derivadas que todos los estudiantes aprenden hoy en día. El cálculo y el algoritmo son las dos ideas más pujantes de la ciencia occidental (Berlinski, 2005)[252]. Leibniz descubrió que si algo tan complicado como la existencia humana podía ser reducido a dos absolutos: Dios y la nada o 0 y 1, ¿por qué el lenguaje no podía ser reconstruido en una manera en que párrafos, oraciones, cláusulas y palabras pudieran ser cernidas para mayor entendimiento? El filósofo y matemático especulaba que los humanos pronunciaban palabras y frases que encajaban en sus percepciones y emociones individuales (Jolley, 1995)[253] . Por su parte, incluso, el Rey Jorge IV fue lo suficientemente inteligente para contratar a Carl Friedrich Gauss en 1817 para analizar el Reino de Hannover (Steiner, 2012). En el S. XVIII, llegaría la forma visual de los algoritmos con científicos como Euler; donde sus gráficos "eran diagramas con forma de árbol que pueden simbolizar redes de la naturaleza, circuitos en un microchip o relaciones entre personas dentro de una ciudad" (Steiner, 2012). Para este autor, " la teoría de gráficos representa uno de los más fascinantes nuevos capítulos de la moderna

[249] Chabert, J.L. ed. Al., (1999) *.A History of Algorithms: From the Pebble to the Microchip*, traducido por Chris Weeks. en Steiner, C.. . *Una breve historia de hombres y algoritmos.* Recuperado de https://catedradatos.com.ar/media/5.-Steiner-Una-breve-historia-de.pdf traducido por Álamo, Alonso y Ortiz.

[251] Bertrand Russel (2008). A Critical Exposition of the Philosophy of Leibniz . New York: Conimo Books, p. 192 en Steiner, C.. *Una breve historia de hombres y algoritmos*.

[252] Berlinski, D. (2005). Infinite Ascent: A Short History of Mathematics. *New york: Modern Library*, p. 45.

[253] Jolley, N. ed.al, The Cambridge Companion to Leibniz. *Cambridge University Press*, 1995, p. 251. ; en Steiner, C.; Una breve historia de hombres y algoritmos.

ciencia computacional, que permite a los biólogos establecer conexiones entre secuencias de ADN y rasgos físicos, a profesores decodificar la música de los Beatles, a la CIA conectar terroristas a lo ancho del mundo, y a los observadores de Wall Street encontrar relaciones entre cosas aparentemente dispares".

Pero, *¿qué es un algoritmo?* La clásica definición de algoritmo dice que un algoritmo es una lista de instrucciones que lleva directamente a un usuario a una respuesta o resultado particular dada la información disponible (Steiner, 2012) [254]. O también se puede encontrar una definición más técnica como "es un constructo matemático con una estructura de control finita, abstracta y efectiva de acción imperativa para cumplir un propósito dada una serie de criterios" (Hil, 2015) [255].

¿Y un *algoritmo médico*? Son algoritmos que basados en computadora ayudan a tomar decisiones médicas o analizar información médica. Por ejemplo, diagnósticos asistidos por computadora a través de imágenes de lesiones de la piel. Se puede decir que hay dos tipos de algoritmo médico: (i) "*algoritmo de investigación*" es el proceso mediante el cual los datos se analizan y se descubren relaciones y (ii) "*algoritmo de predicción"* es el proceso por el cual las relaciones se aplican a nuevos datos para generar predicciones, recomendaciones, y similares (Nichkolson, 2017) [256]. Este autor, resalta la importancia de los algoritmos en el entorno de la salud móvil ("mHealth")[257] , de la que hemos hablado a lo largo de este trabajo[258], principalmente porque la FDA la ha tratado por separado[259], orientado a fines médicos, diagnóstico, tratamiento o bienestar y mantenimiento.

---

[254] Steiener (2012): Automate This: How Algorithms Came To Rule The World, *New York, Portfolio/ Penguin* en; Monasterio A. *Ética algorítmica: Implicaciones éticas de una sociedad cada vez más gobernada por algoritmos*, 2017.

[255] HIL R. (2016): "What an algorithm is?" *Philosophy and Technology* 29 Nº 1 pp. 35-59 en; Monasterio, A. Ética algorítmica: Implicaciones éticas de una sociedad cada vez más gobernada por algoritmos, 2017.

[256] Nickolson Price, W. (2017) II . Regulating Black-Box Medicine" . *Michigan Law Review.* Recuperado de http://michiganlawreview.org/wp-content/uploads/2017/12/116MichLRev421_Price.pdf

[257] Según *Nickolson*, estas aplicaciones "giran en torno a algoritmos integrados, en estos casos, *algoritmos de caja negra*". Es el subconjunto de la medicina algorítmica donde se encuentran los algoritmos inevitablemente opaco, ya sea que esos algoritmos se utilicen en un contexto de mHealth o en otros sistemas, en otras ocasiones no se entiende porque las técnicas de aprendizaje utilizadas no las entiende ni los propios programadores. *Nicholson* señala que "típicamente, los *algoritmos de caja negra* son más valiosos para situaciones en las que las relaciones científicas / médicas subyacentes son especialmente complejas, de modo que identificar y hacer estas relaciones explícitas es demasiado difícil, requiere mucho tiempo o, en muchos circunstancias, imposibles con las herramientas actuales, tales como las relaciones entre miles de genes o redes de factores ambientales".

[258] Cortez, N. (2014). The Mobile Health Revolution? *Law Review University of California Davis*. pp. 1173. Recuperado de https://lawreview.law.ucdavis.edu/issues/47/4/Articles/47-4_Cortez.pdf

[259] Ibíd. pp. 1176.

4.2. Clasificación de IA en salud.

4.2.1. Asistencia de salud móvil ("mHealth")

Mencionamos algunos ejemplos a continuación:

- *Blood pressure monitor.* Aplicación móvil que monitorea frecuencia cardiaca y medición presión arterial[260].

Imagen 27. Blood pressure monitor. Fuente: Blood Pressure Monitor

- *Molly* (Empresa *Sense.ly*). Es una herramienta para la gestión de la salud cuyo interfaz utiliza el aprendizaje automático para apoyar a los pacientes con *enfermedades crónicas* entre las visitas del médico.

Imagen 28. Molly. Fuente: Sense.ly

4.2.2. Asistencia virtual cognitivo dirigido a indivíduos.

El mayor reto estará en la capacidad de estas máquinas para aprender de datos estructurados y genómicos o aprender de datos contextuales y analizar y descifrar lo que dice la gente. A continuación, citamos ejemplos:

- *Pill.* Es un robot asistente que dispensa medicinas, recuerda las dosis de medicina y el momento de la toma y resuelve preguntas sobre salud. Cuenta además con un sistema de reconocimiento facial para identificar a la persona que está realizando la consulta su precio podría estar cerca de los 600 euros.[261]

[260] Vid. https://www.withings.com/us/en/blood-pressure-monitor

[261] Vid. https://www.xataka.com/robotica-e-ia/pillo-es-robot-asistente-que-mira-por-tu-salud-reconoce-caras-y-dispensa-medicamentos


Imagen 29. Pill robot. Fuente: Xataka

- *Ping An Good Doctor*[262]. Se trata de un doctor virtual con IA que utiliza datos procedentes de 300 millones de consultas previas y recopila interactuando a través de texto y voz todos los síntomas y el historial médico del paciente y hace una sugerencia diagnóstica preliminar. A continuación, un médico real mediante videoconferencia supervisa o corrige las conclusiones de IA y aporta comentarios complementarios. Hace poco pusieron un proyecto piloto: una cabina pública abiertas las 24 h. donde se proporcionaba atención médica sin necesidad de personal médico presencial.


Imagen 30. Ping an good doctor. Fuente: Xataca

- *Bodyo*[263] *(Dubai).* Se trata de cápsulas de IA de Escáner digital AI Pod de autoservicio que permite 19 mediciones rastrando indicadores de salud vitales en sólo 10 minutos. Éstas están instaladas en centros comerciales o supermercados.

---

[262] Vid. https://m.xataka.com/inteligencia-artificial/compania-china-proporciona-consultas-medicas-sustituyendo-personal-medico-asistentes-virtuales/amp. Se trata de una plataforma de atención médica con 228 millones de usuarios registrados. Ya se han instalado también en grandes y medianas empresas, grandes comunidades de viviendas, cadenas de farmacias y otras áreas concurridas, con lo que llegaran a ser hasta ciento de miles de cabina.; Ver también, VIDAL, Marc (29 de marzo, 2019), para ver vídeo de *Ping an good Doctor*: https://www.linkedin.com/feed/update/urn:li:activity:6517335238446714880/

[263] Me parece interesante detenernos en las interesantes líneas de negocio de esta empresa:

a. *Para aseguradoras.* Señalan: "Los investigadores estiman que el 75% de todos los costos de atención de la salud son directamente atribuibles a enfermedades crónicas prevenibles, como la obesidad, la hipertensión y la diabetes tipo 2. BodyO es un sistema integrado clave para recopilar y monitorear información de salud esencial con recomendaciones para un plan efectivo de ejercicio y nutrición."
b. *Para corporaciones*. Señalan:"BodyO es una solución esencial que le ayuda a desarrollar un programa de bienestar corporativo eficaz. Los usuarios serán: (i) Reducir el absentismo laboral; (ii) Disminuir el nivel de estrés; (iii) Menores costos de cuidado de la salud y de seguros; (iv) Aumentar la retención de los empleados; (v) Mejorar la moral de los empleados; (vi) Aumentar la productividad; (vii) Aumentar la motivación de los empleados (viii) Aumentar la motivación para practicar comportamientos saludables".
c. *Para profesionales.* Señalan; "BodyO ofrece a los entrenadores, nutricionistas, médicos y profesionales de atención domiciliaria la capacidad de realizar un seguimiento y medir los aspectos vitales de sus clientes y pacientes a través de una plataforma de atención médica innovadora e integrada. La plataforma también ofrece un registro de salud y entrenamiento basado en la nube, el registro de calorías, lípidos y proteínas, un acceso a 1,000 ejercicios de acondicionamiento físico y 20,000 recetas culinarias"
d. *Para instituciones de salud.* Señalan; "BodyO es la solución perfecta para hospitales, clínicas y centros de bienestar para realizar un seguimiento de los signos vitales de sus pacientes y asegurarse de abordar los problemas en el momento adecuado":

Imagen 31. Bodyo. Fuente Bodyo

Pero además, se trata de IoT, IA y Blockchain con "body health utility token". Cuentan con un contrato inteligente entre un sistema de recompensa alojado y un paciente publicado en la cadena de bloques. Los pacientes que muestran un buen comportamiento son recompensados con este token.

4.2.3. Asistencia o personal sanitario[264].

- *Lumiata.* Pueden transformar *datos de reclamaciones de seguros, registros médicos, sensores médicos y otras fuentes en información* que se puede usar para predecir las mejores formas de tratar pacientes y condiciones individuales. Los algoritmos de la compañía integran datos de muchas fuentes con información medida directamente en o proporcionada por el paciente, incluyendo, potencialmente, a través del uso de monitores de paciente portátiles[265], para proporcionar diagnósticos, predicciones y recomendaciones de tratamiento sugeridos por los individuos. El sistema de Lumiata también sugiere análisis de todo el sistema, que ayuda a los hospitales a asignar recursos a los pacientes que más los necesitan, y también ayuda a los hospitales a detectar oportunidades de facturación sin aprovechar"[266].

- *Deep Genomics.* Identifica patrones en enormes conjuntos de datos de *información genética y registros médicos*, en busca de mutaciones y vínculos con la enfermedad. Asiste a los médicos y les informa lo que sucederá dentro de una célula cuando el ADN es alterado por la variación genética, ya sea natural o terapéutica.
- *AiCure.* Es una herramienta de seguimiento médico que a través de cámara web de un smartphone y la inteligencia artificial confirma *de forma autónoma* que los pacientes están

---

e. Para gobiernos. Señalan: "Tener BodyO en una institución del gobierno médico puede conducir a la prevención de enfermedades graves como hipertensión, hipercolesterolemia, diabetes tipo II, accidentes cerebro vasculares, obesidad mórbida y algunos tipos de cáncer".

[264] Nos referimos a las *consultas en línea o presenciales* en casos de síntomas simples donde el software puede darle respuestas basadas en sus registros médicos o a los *asistentes cognitivos* que ayudan al personal médico a tomar decisiones clínicas con el uso de datos e informes a través del escaneo de imágenes de radiología para detectar un problema.

[265] Scott Amyx, Wearing Your Intelligence: How to Apply Artificial Intelligence in Wearables and IoT, Wired (2014) Vid. https://www.wired.com/insights/2014/12/wearing-your-intelligence/ en . NICKOLSON PRICE (2017) II "Regulating Black-Box Medicine".

[266] Vid. https://www.lumiata.com/# en . NICKOLSON PRICE (2017) II "Regulating Black-Box Medicine".

cumpliendo sus prescripciones o con mejores términos. Está apoyada por los Institutos Nacionales de la Salud.

- *Human Longevity*[267]. Ofrece a sus pacientes la *secuenciación completa del genoma*, junto con una exploración completa del cuerpo y un chequeo médico muy detallado. Todo el proceso permite detectar el cáncer o las enfermedades vasculares en su etapa muy temprana[268].

- *Algoritmos de investigadores de Stanford*. A partir de la visualización de la radiografía, calcula el nivel de probabilidades de desarrollo de neumonía en el paciente, creando un mapa de calor indicando las áreas que llevan a esa conclusión. Se ha tomado base de datos de 30.000 pacientes[269].

- *Deep Patient*[270]. Donde se utiliza el *Deep learning*, un enfoque de aprendizaje automático que básicamente " imita las redes neuronales del cerebro", permitiendo que el sistema informático aprenda cosas nuevas sin estar programado para hacerlo. Un estudio de Google sobre gatos en 2012 ilustra el concepto de aprendizaje profundo. Después de escanear millones de fotos, una red neuronal computarizada logró casi el 75% de precisión en la identificación de los gatos, sin recibir ninguna información sobre los gatos o los rasgos del gato. Ahora, el experto Dudley quiere llevar ese tipo de aprendizaje a la práctica médica. Con *Deep Patient,* los científicos alimentaron datos no identificados de *700,000 registros médicos en una red neuronal computarizada*, *que combinó datos aleatoriamente para crear y probar nuevas variables para el riesgo de enfermedad.* La esperanza era que la máquina podría entrenarse para comprender todos los datos de una manera que facilitara el modelado predictivo. En un estudio[271] de 2016 publicado en *Científica Reports* , Dudley y sus colegas evaluaron a *Deep Patient* recién formado que usaba más de 76,000 pacientes de prueba que tenían 78 enfermedades. Descubrieron que *Deep Patient* "significativamente mejoró" las evaluaciones basadas únicamente en datos de EHR sin procesar, lo que le permite predecir especialmente la diabetes grave, la esquizofrenia y varios cánceres[272].

---

[267] Al mismo tiempo, el dueño de la empresa, *Craig Venter*, uno de los padres del Proyecto del genoma humano está trabajando en un algoritmo que podría diseñar las características físicas de un paciente basado en su ADN.

[268] Ver en https://www.merca2.es/la-inteligencia-artificial-cuidado-medico/

[269] Ver en https://wwwhatsnew.com/2017/11/17/este-algoritmo-puede-detectar-neumonia-con-mas-precision-que-un-radiologo/?utm_source=dlvr.it&utm_medium=twitter

[270] Ver https://news.aamc.org/research/article/artificial-intelligence-transforms-future-medicine/

[271] Ver https://www.nature.com/articles/srep26094

[272] Así por ejemplo, *Regina Barzilay,* PhD (MIT) dirige un proyecto de IA para el cáncer donde se utiliza el procesamiento del lenguaje natural para enseñar a las computadoras cómo leer e interpretar los datos de EHR, incluidas las partes no estandarizadas conocidas como texto libre. En otras palabras, los algoritmos aprenden lea los informes de patología mamaria e identifique con precisión si hay cáncer presente. Eso es un gran problema, según Hughes, porque significa que los investigadores y los médicos pueden usar AI para ordenar e identificar franjas masivas de datos de patología relevantes que alguna vez fueron inteligibles para los humanos, y que tienen el potencial de revelar nuevos conocimientos sobre prevención y detección del cáncer. y tratamiento

- *Human Diagnosis Project (Human Dx)*. En la actualidad, un médico de atención primaria utiliza el sistema eConsult para hablar sobre un caso particular de un paciente con un especialista en lugar de derivar al paciente a una visita en persona. Bajo la asociación Project CORE-Human Dx, A*I eventualmente permitirá que los médicos de atención primaria envíen un eConsult y reciban consenso de múltiples especialistas simultáneamente.*

- *Retinalyze*[273]. Se ha desarrollado un algoritmo aplicado a un software de análisis en tiempo real que detecta de forma automática y precoz lesiones del ojo vinculadas a las tres enfermedades más frecuentes causantes de la ceguera como el glaucoma, la degeneración macular y la retinopatía diabética. La plataforma se encarga de procesar estas imágenes y trasladarlas a la nube, desde donde un algoritmo detecta de forma automática lesiones oculares.

- *Facebook y Universidad Nueva York*[274]. Se trata de un software de inteligencia artificial con una base de datos que incluye más de 1,5 millones de imágenes de aproximadamente 10.000 escaneos, 1.600 de las exploraciones vienen con varios datos de medición anatómica. Todas las exploraciones tienen información del paciente eliminada de forma permanente y la base de datos es totalmente compatible con la HIPAA estadounidense, ahora bien, ambos han afirmado que "no se utilizan datos de ningún tipo de la red social en el proyecto".

- *Universidad de Carolina del Norte* (*Lineberger Comprehensive Cancer Center)* - Watson[275]. La tecnología encontró opciones de tratamiento que los médicos habían pasado por alto basadas en investigaciones que los médicos no habían leído o ensayos que no conocían.

4.3. Riesgos y la protección de datos

Es importante, antes de continuar con el estudio, detenernos en las diferencias existentes entre 3 conceptos: "*analytics bigdata*" y "machine learning" y *"deep learning":*

Analítica de datos o análisis predictivo *("analytics data")*	**Aprendizaje automático** *("machine learning")*	**Aprendizaje neuronal** *("deep learning")*
Hablamos de utilización de Big Data o datos	Es un sistema de	Es un sistema de Inteligencia

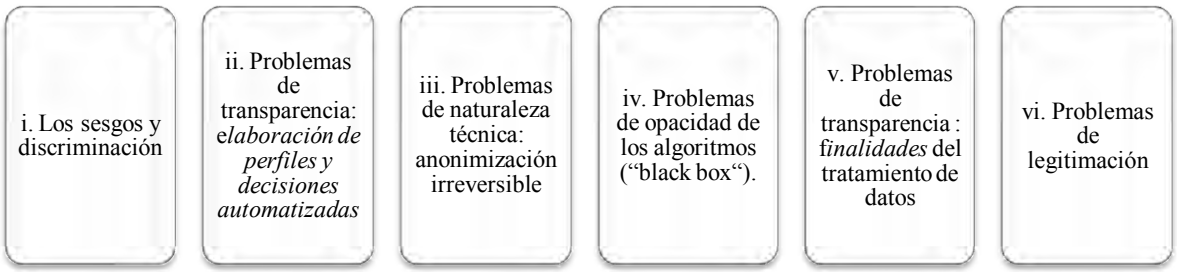
[273]Ver https://www.consalud.es/saludigital/112/nuevo-algoritmo-de-ia-para-detectar-enfermedades-oculares_50701_102.html
[274]Vid.https://www.consalud.es/saludigital/134/facebook-crea-una-base-de-datos-de-imagenes-de-resonancias-magneticas_57657_102.html
[275] Vid . https://unclineberger.org/

masivos donde se pueden incluir datos personales de salud. Es el procedimiento para condensar grandes volúmenes de datos. Depende de personas para trabajar. Incluyen promedios y recuentos basándose en eventos pasados para predecir eventos futuros. Ej. ¿Cuántos pacientes de gripe habrá este invierno teniendo en cuenta que…? Elementos: a.) Datos. Dependen de la calidad de los datos. b.) Modelo estadístico. Incluye técnicas estadísticas con funciones básicas o complejas. c.) Suposiciones. Son conclusiones extraídas de los datos recopilados y analizados.	Inteligencia Artificial. Es una rama de mejora del análisis predictivo. Resuelve predicciones. No depende de personas. Los sistemas de algoritmos mejoran a través de la experiencia de datos sin depender de programación externa. Realizan predicciones a la vez que mejoran sus sistemas.	Artificial. Por ejemplo, el caso de IA en reproducción asistida (Universidad Columbia[276]). Es más complejo, más autónomo, mas sofisticado. La diferencia con el anterior es la forma del aprendizaje. Lleva el aprendizaje a un nivel superior y va por capas o redes neuronales. Es un sistema que trata de imitar al cerebro. Intenta reducir el error al mínimo posible. Son capaces de resolver problemas creando nuevas alternativas o estrategias. Ej. Al sistema le da igual que en los registros médicos o en las escáneres o radiografías aparezca nublada una muestra poniendo en duda si se trata de un fémur o un radio porque ya sabe lo que es uno y lo que es otro.

Tabla 16. Tabla comparativa analítica datos, machine learning y deep learning. Fuente propia.

Como podemos ver la primera se refiere las técnicas analíticas que se usan en la tecnología big data, en las otras dos, se refieren a sistemas de IA diferentes entre sí. Esto hay que tenerlo en cuenta para determinar los riesgos en materia de protección de datos y privacidad que puedan surgir. A continuación, mencionaremos cuestiones que generan esos riesgos en el ámbito de la IA en salud:

[276] Vid. https://www.nature.com/articles/s41746-019-0096-y



i. Los sesgos y discriminación en el tratamiento de datos.

También es un reto para IA, no sólo para Big Data, no olvidemos que pueden considerarse como tecnologías complementarios. La consideración general 19 de la Resolución del Parlamento Europeo sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI)) [277] ya indicaba que;

> "como consecuencia de los conjuntos de datos y *sistemas de algoritmos* que se utilizan al hacer evaluaciones y predicciones en las distintas fases del tratamiento de datos, los macrodatos no solo pueden resultar en violaciones de los derechos fundamentales de los individuos sino, también, en un tratamiento diferenciado y en una *discriminación indirecta de grupos de personas con características similares*, en particular en lo que se refiere a la justicia e igualdad de oportunidades en relación con el acceso a la educación y al empleo, al contratar o evaluar a las personas o al determinar los nuevos hábitos de consumo de los usuarios de los medios sociales (o incluso en base a la raza[278] o el sexo[279])".

Cathy O`Neil[280], ex analista de Wall Street y autora del libro "Armas de destrucciónn matemática", indica que existen algoritmos que se basan en estadísticas falsas o sesgadas que fomenta la desigualdad y la discriminación. Este reto nos puede derivar a otro reto ; el de las clásicas *elaboraciones de perfiles grupales y a las decisiones automatizadas* que se llevan a cabo cada día en el sector financiero, de la sanidad, etc.

ii. Problemas de transparencia: elaboración de perfiles y decisiones automatizadas.

[277] *Supra. Cit.*
[278] Vid. Rabess, Cecilia Esther (2014) Can big data be racist? *The Bold Italic*, http://www.theboldditalic.com/articles/4502-can-big-data-be-racist
[279] Vid. Sweeney, Latanya (2013). Discrimination in online ad delivery. *Data Privacy Lab* http://dataprivacylab.org/projects/onlineads/1071-1.pdf
[280] BBC (1 de noviembre de 2016). Los algoritmos ocultos que funcionan como "armas de destrucción matemática. *BBC news.* Recuperado de http://www.bbc.com/mundo/noticias-37837377.

En ocasiones los algoritmos son *opacos y secretos* y no siempre los titulares de los datos conocen las finalidades de cualquier tipo de tratamiento que van a recibir de sus datos.

Como señala la Comisión Europea[281], se considera que se elaboran perfiles cuando los aspectos personales son evaluados para elaborar predicciones sobre la persona, incluso si no se toman decisiones. Por ejemplo, si una empresa u organización evalúa características (como la edad, el sexo, la altura) o incluye a ese individuo en una categoría, significa que se está elaborando un perfil sobre el mismo. Y se puede ir más lejos ; cuando esa empresa toma decisiones por medio de modelos matemáticos donde no participan humanos. Por ejemplo, Un individuo quiere contratar una póliza de seguro a aseguradora de salud . Se le pide que introduzca sus datos y el algoritmo de la aseguradora le dice si el ésta le concederá el seguro o no y le sugiere un tipo de prima. La aseguradora "deberá informar de que puede expresar su opinión, *impugnar la* decisión y solicitar la contribución de una persona en el proceso para revisar la decisión tomada mediante el algoritmo" "(Comisión Europea).

No obstante, el legislador intentando para evitar que pudieran producirse vulneración del derecho fundamental del individuo , crea el art. 22 RGPD para prohibir de manera expresa estas decisiones automatizadas:

> *"Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar."*

La prohibición se aplica a las decisiones que se basan " *exclusivamente* " en el procesamiento automatizado, pero como destaca el GT 29[282], "*la supervisión humana de la conclusión a la que llega la máquina debe ser significativa"* **.** De lo contrario, sería solo una forma de eludir la prohibición.

Las excepciones de aplicabilidad no directa dicha regla se aplican cuando una decisión automatizada:

a. es *provista por la ley*, como en el caso de los controles de prevención de fraude o de lavado de dinero,

[281] Vid. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-be-subject-automated-individual-decision-making-including-profiling_es

[282] Vid. Directrices del GT29 sobre decisiones individuales automatizadas y perfilado a los efectos del Reglamento (UE) 2016/679 (WP 251).

b. es *necesaria*[283] para la ejecución o celebración de un contrato, (piénsese en marketing con datos que no son de salud),
c. se basa en el *consentimiento previo del individuo*[284].

Además, el RGPD requiere que se informe dando detalles sobre:

a. el *uso las tecnonologías de IA y machine learning*;
b. la *importancia y las consecuencias* previstas para el individuo;
c. la *información significativa* sobre la lógica involucrada**.**

De acuerdo con el GT29, la explicación de la lógica involucrada incluiría detalles sobre la razón de ser o los criterios en los que se basa para tomar la decisión**,** evitando una explicación compleja de los algoritmos utilizados. En la política de privacidad se podrían incluir las principales características consideradas al tomar la decisión, la fuente de esta información y su relevancia.

A continuación, vemos un ejemplo de aseguradora digitalizada ("*Vivaz", de Linea Directa*) y una parte de su política de privacidad, quien explica de forma breve y clara la relevancia por el que se realizan estas decisiones automatizadas; "para fijar la tarifa más baja ajustada a las condiciones de su persona…".

[283] Llamemos la atención que esto no tendría cabida para datos de categoría especial como son los datos de salud. En todo caso, del mismo modo y según las autoridades de protección de datos de la UE, la interpretación de " *necesidad* " para la entrada en un contrato debe interpretarse de manera restrictiva. En particular, " *el responsable debe poder demostrar que este perfil es necesario, teniendo en cuenta si se puede adoptar un método menos intrusivo para la privacidad* ".

[284] Ahora bien, ¿qué pasaría si *añadimos la institución del consentimiento previo* en el tratamiento de datos personales en esta tecnología sería una opción viable? A priori, puede parecer difícil creer que los individuos otorguen su consentimiento. Además hay que tener presente el problema que surge cuando los sistemas de decisión automatizados se utilizan para procesar categorías especiales de datos, como datos relacionados con la salud. En ese caso, el *RGPD no prevé la excepción a la prohibición vinculada a la necesidad de cumplir o celebrar un contrato* (entiendo que sin que haya una supervisión humana a la conclusión que lleva la máquina**).** Es obvio pensar que en situaciones donde las aseguradoras puedan procesar automáticamente los datos de salud de las personas para evaluar el riesgo del seguro ponen en riesgo al derecho y libertad de éstas para decidir si desean o no dar su consentimiento (en el tratamiento automático de sus datos de salud) y puede acarrear un alto precio a su derecho fundamental de protección de datos**.**

¿Por qué a veces es preciso elaborar perfiles y adoptar decisiones automatizadas?

- Como se ha expuesto, para fijar la tarifa más baja ajustada a las condiciones de su persona, es preciso tomar decisiones basadas en el análisis automatizado o informático de los datos que nos ha entregado, o de los ficheros a los que se puede acceder para ello. La lógica de dichas decisiones es la de poder atender de forma ágil y objetiva a todas las personas en los procesos de contratación y renovación de los seguros, ponderando así las mismas circunstancias para todos, de manera informática.
- Del mismo modo, las normas de solvencia de una aseguradora obligan a realizar estudios estadísticos y perfiles sobre cada asegurado, para adelantarnos y prever la probabilidad de que suceda un siniestro. De esta forma, para garantizar su pago, se pueden dotar provisiones contables adecuadas (reservas de dinero previstas para el abono de siniestros). Para ello es preciso adoptar decisiones complejas a nivel informático y crear perfiles de asegurados con los que gestionar los riesgos objeto de coberturas.
- Finalmente, la mercadotecnia moderna implica realizar ofertas y descuentos ajustados a su perfil particular, ajustes que precisan del análisis de las circunstancias concretas de cada persona a través de herramientas informáticas.

Imagen 15. Clausula informativa respecto a perfiles y decisiones automatizadas de la aseguradora Fuente: Vivaz

Pero ahora bien, el derecho a la oposición ("y al derecho de intervención humana") de estos tratamientos debe ser claro e informado al potencial asegurado. Así lo realiza:

En los casos de decisiones basadas únicamente en decisiones automatizadas que produzcan efectos jurídicos en usted o que le afecten de significativamente de forma similar a dichos efectos jurídicos, tiene derecho a obtener intervención humana en tal decisión, así como a expresar su punto de vista, pudiendo si lo desea impugnar tal decisión.

Imagen 16. Clausula informativa respecto al derecho de oposición en perfiles y decisiones automatizadas de la aseguradora Vivaz

Ahora bien, los individuos podrán impugnar la decisión o a recibir una justificación de la decisión automatizada. Imaginemos el caso de un contrato de seguro de salud donde el sistema rechaza la solicitud al no cumplir ciertos parámetros (ej. no alcanza cierto número de pasos al día según su dispositivo *wearable fitbit*). Pero, ahora bien, ¿de qué manera se debe justificar y hasta qué punto llegar con dicha justificación? ¿deberán explicar los "árboles de decisión" que posibilitan la "ruta de aprendizaje"? ¿cómo? Las empresas aún no saben como están aprendiendo las máquinas más complejas por lo que mucho menos podrán explicarlo a los individuos.

El problema viene cuando el sistema IA se vuelve tan complejo que sus decisiones se basan en una gran cantidad de datos que no es posible dar esa justificación de la decisión automatizada (o sistemas neuronales de *deep learning*). Es obvio, además, que estos últimos acarrean mayores riesgos por su naturaleza técnica; son autónomos y no necesitan de intervención humana por lo que hace pensar que los tratamientos automatizados en estos sistemas no estarán permitidos por la legislación comunitaria.

Imagen 32. Evolución tipos IA.

iii. Opacidad de los algoritmos ("black box") en los IA deep learning.

Es de mencionar los siguientes extremos;

- *Problemas de transparencia general.* Las empresas no saben qué sucede y qué razonamiento hay detrás del resultado. Los algoritmos son impredecibles.
- *Solución:* Los científicos de datos de las empresas deberán acercar lo máximo posible a la transparencia para que los individuos estén informados. Por ejemplo, Pretzel[285] es un sistema de servicio de predicción que presenta una arquitectura de caja blanca novedosa que permite optimizaciones de extremo a extremo y de múltiples modelos. Introducen tuberías con mejoras de rendimiento en diferentes dimensiones. Se tardarán años hasta conseguir dicha transparencia que permita cumplir con el RGPD[286].
- *Repercusiones de una mayor transparencia.* Según los expertos de ciberseguridad de IA, dedicar más recursos en este ámbito supone dedicar menos recursos para realizar sistemas más efectivos y precisos

iv. Problemas de naturaleza técnica: anonimización irreversible.

En los sistemas IA, no siempre hay ggarantías suficientes para el uso de datos personales de salud con fines estadísticos o científicos. Nos referimos a que se producen disociaciones deficientes o reversibles que permiten la re-identificación de datos de categorías especiales en procesos de investigación que solo prevén utilizar datos anónimos.

v. Problemas de transparencia: finalidades del tratamiento de datos.

Los sistemas de IA se basan en el procesamiento de una gran cantidad de datos provenientes de diferentes fuentes y garantizar que el fin del tratamiento de datos es el inicial y no otro, resulta complicado. Por ejemplo piénsese en escenarios donde exista utilización de metadatos de salud (ej. llamadas de emergencias de suicidio) sin haber declarado o existan decisiones automatizadas o profiling con supervisión significativa humana sin haberlo comunicado al titular. En todo caso, siempre será necesaria la

---

[285] Lee, Y. et. Al. (2018). PRETZEL: Opening the Black Box of Machine Learning Prediction Serving Systems. *aeXiv of Cornell University*. Recuperado de https://arxiv.org/abs/1810.06115

[286] Burlacu, A. (12 de agosto de 2018). Understanding a Black-Box. *Towards Data Science*. Recuperado de https://towardsdatascience.com/understanding-a-black-box-896df6b82c6e

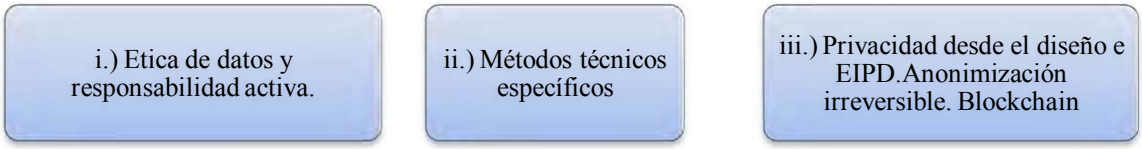
transparencia por parte responsables y encargados aplicando recomendaciones que indicábamos en el caso de la tecnología *big data.*

vi. Problemas de legitimación del tratamiento de datos.

Nos referimos a fallos o errores sistemáticos u ocasionales para recabar el *consentimiento expreso* al ser ésta la base legítima. Según *David Gray*[287], lo que podría ser una solución es contar con IA con *"código abierto"*. Por ejemplo, pensemos en una app de *e-Health* ("app Vida") la cual utiliza esta tecnología donde pregunte acerca del consentimiento para reunir y combinar datos. En este caso el individuo puede no dar el consentimiento pero sólo podría otorgarlo en situaciones donde su ritmo cardiaco fuera bajo y sugiera un accidente de tráfico. A medida, que los sistemas de IA ganen autonomía y se acerquen a *"deep learning",* sus dispositivos tendrán capacidad de preguntar al individuo si da su consentimiento para el tratamiento de los datos datos que él considere (quizás no quiere que se traten sus datos biométricos o genéticos). En otros casos, se puede dar la asunción errónea de la existencia de una habilitación legal para el tratamiento o cesión de datos de la categoría especial de los datos de salud (ej. a través de interés legítimo) o la cesión a terceros (ej. a empresas de la industria farma). También se pueden dar accesos no autorizados a datos personales a personal de la empresa responsable que no está autorizada.

4.4. Una aproximación a posibles soluciones

A continuación hablaremos de las siguientes opciones;



i. Ética de datos y responsabilidad activa.

[287] Ver en : https://www.enterpriseirregulars.com/116296/%E2%80%8Bartificial-intelligence-privacy-engineering-matters-now/

La ética[288] otorga la mayoría de las soluciones a las tecnologías emergentes como veremos con más detalle en los capítulos próximos. Por el momento, conviene que nos planteemos , ¿es compatible el sistema IA con el RGPD? ¿está el flujo de información de datos personales en el sistema bajo control y cumple con RGPD? ¿cómo pueden los individuos buscar información sobre un consentimiento válido y cómo se puede revocar dicho consentimiento? Etc.. Por otro lado, cuando nos referimos a responsabilidad activa nos referimos a que responsables y encargados de tratamiento usen medidas técnicas y organizativas según RGPD (art. 32 y 35) incluidas técnicas de cifrado y anonimización, que se realicen homologación previa del proveedor de los servicios IA y los subproveedores (análisis de clausulas contractuales, auditorías, certificaciones, adhesión a códigos de conducta), o que se incluyan clausulas de penalización ante incumplimiento

ii. Métodos técnicos.

Nos referimos, principalmente a los métodos que indica el *borrador de Directrices de ética para IA confiable (Draft Ethics Guidelines for trustworthy AI)*[289]; ética por diseño, arquitecturas para IA confiables, pruebas y validación, trazabilidad y auditabilidad y explicación. Además, recientemente, también la FDA[290] norteamericana ha creado una guía para cambios de diseño en el software de los dispositivos médicos. Por su parte, Nick Bostrom (2014), habla de *técnicas de control y seguridad* en IA avanzada que prevenga un uso instrumental de los seres humanos por parte de una Súper-Inteligencia. En el futuro, los sistemas tenderán a ser sistemas "deep learning" más autónomos y sofisticados, no será tarea fácil hacerlo encajar con el marco jurídico actual. Aunque, quizás, estos sistemas aprender a "eliminar" de forma autónoma y

[288] Elish, M.C. (2016). Moral Crumple Zones: Cautionary Tales in Human-Robot Interation. En We Robot Conference Paper Draft. Recuperado de http://robots.law.miami.edu/2016/wp-content/uploads/2015/07/Elish_cautionary-tales_prelim_draft.pdf . En verdad, se necesitaría prácticamente de un equipo de personas que vigilara lo que hace la máquina en relación con los datos que fueron tratados (David Gray, 2017). Lo que Michelle Deneddy aconseja es crear zonas de deformación éticas *("moral cumple zones")* (Elish, 2016). Para la autora, "el humano en un sistema robótico puede convertirse simplemente en un componente, accidentalmente o intencionalmente, que está destinado a soportar la mayor parte de las sanciones morales y legales cuando falla el sistema en general" , como si se tratara de un sistema de rendición de cuentas prácticamente.

[289] Ver https://ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai

[290] Ver https://www.regulations.gov/document?D=FDA-2019-N-1185-0001 ; ver también https://www.statnews.com/2019/04/02/fda-new-rules-for-artificial-intelligence-in-medicine/

automática los datos personales aplicándose una especie de "olvido selectivo" (ej. datos personales de categoría especial que sean identificativos) .

iii. Privacidad desde diseño y EIPD. Anonimización irreversible. Blockchain.

Se esperan las medidas que se implanten desde el momento inicial *del diseño* del sistema IA, que propone el legislador en el RGPD, como son la *anonimización irreversible* para proteger datos de especial categoría como son los datos personales de salud. También prevé de forma expresa el legislador en el considerando 71 cuando establece claramente que el responsable de tratamiento debería usar procedimientos matemáticos o estadísticos apropiados para perfilando y tomar medidas para prevenir la discriminación en el por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, estado genético o de salud o orientación sexual". Da vía libre al responsable del tratamiento para que con ciertos procedimientos evite la discriminación por motivos de estado genético o de salud. Además, el regulador europeo encuentra entre una de las medidas reforzadas nuevas, la *evaluación de impacto de protección de datos (EIPD)*[291]. Aparece un concepto que merece ser destacado; "*obscurity by design*" (Hartzog, 2013)[292]. Su autor propone "soluciones basadas en el diseño para tecnologías sociales que se beneficien de una mayor atención a la interacción del usuario, con un enfoque en los principios de oscuridad en lugar del concepto vago y expansivo de privacidad".

Al igual que planteé el recurso de la *tecnología blockchain/DLT* en big data, quisiera extenderlo a los sistemas IA. Cuando se combina con blockchain[293] , la IA puede ser

---

[291] Se trata según el RPGD " *una evaluación sistemática y exhaustiva de los aspectos personales relacionados con las personas físicas que se basa en el procesamiento automatizado, incluida la elaboración de perfiles , y en la que se basan las decisiones que producen efectos jurídicos respecto de la persona física o afectan significativamente a la persona física* "Es importante destacar que la disposición anterior no se refiere solo a las evaluaciones que se basan "exclusivamente" en el procesamiento automatizado. Por lo tanto, será necesario un DPIA en caso de cualquier perfil automatizado ejecutado mediante IA, machine learning u otras tecnologías capaces de producir efectos en los individuos, incluso si existe una intervención humana en la evaluación de los resultados de las máquinas. Esto representa una obligación bastante onerosa, pero especialmente a la luz del principio de responsabilidad, es una protección bastante relevante en caso de reclamaciones. De hecho, una evaluación de impacto de privacidad mostrará que el responsable del fichero o del tratamiento consideró todos los factores involucrados y estableció protecciones adecuadas de los derechos de privacidad de las personas.

[292] Vid. Hartzog, W., Stutzman, F.D. (2013) . Obscurity by Design, *Washington Law Review*, Vol. 88, 386. Recuperado de https://ssrn.com/abstract=2284583. (Sin duda, uno de los mayores problemas existentes tienen que ver con lo que denominan como *"obscurity by design de los algoritmos"*. . La oscuridad, por tanto, "es la protección óptima para la mayoría de las interacciones sociales en línea y, como tal, es un lugar natural para soluciones de privacidad basadas en diseño para tecnologías sociales").

[293] Vid. https://blog.oceanprotocol.com/blockchains-for-artificial-intelligence-ec63b0284984

mejor comprendida por los humanos y funciona de una forma más eficiente. Cuentan con un contrato inteligente entre un sistema de recompensa pacientes con buen comportamiento de salud. Como explican *Tshilidzi Marwala y Bo Xing*[294] , hay ocho formas clave en que la IA puede ayudar a las cadenas de bloques. Las funciones de seguridad y privacidad, escalabilidad y eficiencia son las más relevantes por cuanto nos interesa en este trabajo. Por ejemplo, *Bodyo (Dubai),* como hemos dicho a lo largo del trabajo se trata de un sistema con tecnologías combinadas IoT, IA y Blockchain con "*body health utility token"*.

Imagen 31. Bodyo. Fuente Bodyo

En el ámbito de la atención sanitaria, tal y como señala *Carretero et. al.* (2018)[295] :

> "Las ventajas de la aplicación de *técnicas de IA* como sistemas avanzados en la gestión del conocimiento, validación de evidencias, descubrimiento de indicios, así como la creación de sistemas de apoyo a la decisión en la eficiencia diagnóstica y terapéutica, está sobradamente demostrada con los cientos de "papers" que se publican diariamente al respecto. Y sin embargo, sigue existiendo *un problema insalvable en la excelencia analítica,* principalmente en el contexto de la salud: *poder disponer de datos de calidad, desagregados y compartidos por todos los centros de salud a nivel mundial: hospitales, laboratorios, bancos de tejidos y centros de investigación".*

Por tanto, blockchain podría cubrir esas cuestiones que no alcanza la tecnología IA:

> "…imaginen un sistema en el que la información se registra de forma distribuida, codificada, en un entorno global, en el que, a pesar de que existan distintas codificaciones (*UMLS, Cie-9, CIE-10, Snomed, Hl7,…),* ciertos agentes son capaces de negociar los contenidos llegando a acuerdos de codificación universales y estandarizados, y en el que la información que se mantiene es segura: sólo aquellos que tienen acceso a la misma pueden recuperar parte de dicho conocimiento, y no existen intermediarios entre los agentes.
>
> Aunaríamos el valor de la "Internet del Conocimiento" (web semántica), con la "Internet del Valor" (Blockchain), en el sueño de la mayoría de los investigadores, disponer del mayor nivel de conocimiento sobre el mayor número de pacientes y el mayor número de contextos médicos.

[294] Marwala, T., Xing, B. Blockchain and AI. University of Johannesburg. Recuperado de https://arxiv.org/ftp/arxiv/papers/1802/1802.04451.pdf

[295] Carretero, P.; de la Peña , P; Moreno Fdz., Aitor; (2018) . Blockchain en Sanidad. *Revista de la Sociedad Española de Informática y Salud.* Blockchain en salud. ¿Realidad o quimera?. Núm., 128. PP. 15-7. Recuperado de https://seis.es/wp-content/uploads/2018/04/128.pdf pp17.

> Blockchain, con sus propiedades en cuanto a la privacidad y a los contratos inteligentes, permitiría disponer de toda esa información resolviendo *el problema de la interoperabilidad* en una única plataforma.[296]

Según estos autores, "el prometedor futuro sólo puede provenir de la unión de los tres grandes hitos de la nueva tecnología: la Inteligencia Artificial, la Semántica y el Blockchain".

5. BLOCKCHAIN Y DLT EN SALUD.

Actualmente la industria de la tecnología se valora en unos 385,5 millones de dólares[297]. Una investigación[298] reveló increíbles predicciones para la industria del blockchain, en concreto, un crecimiento anual compuesto del 74,1%, equivalente a 28 millones de dólares para el 2025. El blockchain en el mercado sanitario se espera que se valore $ 5,61 mil millones para 2025.Tomando una visión más amplia, se estima que el mercado global de datos médicos valdrá $ 14 mil millones en 2017, y se proyecta que llegará a $ 69 mil millones para 2025, impulsado por una mayor adopción de almacenamiento en la nube, iniciativas gubernamentales a gran escala y una creciente demanda de dispositivos portátiles. Con respecto a esto último, McKinsey estima que para el año 2025, alrededor de 1.3 mil millones de monitores de estado físico estarán en uso en todo el mundo.

[296] *Carretero et. al.* (2018) señalan que "extraer el conocimiento de esta ingente fuente de datos, de una forma segura y anónima, sólo se puede hacer de una manera, generando algoritmos de extracción inteligente (los actuales algoritmos de minería de datos), pero desde el interior de las cadenas de Blockchain. De esta forma, *los datos no saldría nunca fuera de la cadena*, sólo suministraríamos a nuestros consumidores agregados, patrones y perfiles de pacientes, y las reglas de cuáles son las mejores terapias para cada perfil, de una forma agregada, y en forma de conclusiones, evidencias o indicios". "Así*, la empresa que consiga aplicar mejores algoritmos de pronóstico o de perfilado internamente sobre los datos de las cadenas, será la que más venda sus conclusiones a terceros,* en un nuevo paradigma de "app store" del conocimiento más valor".

[297] Todo ello gracias a una mayor adopción de las BaaS *(Blockchain as a service) como* también el incremento de interés de los comerciantes en las monedas digitales traduciéndose en un aumento de confianza del consumidor. Además compañías (minoristas) como PayPal, Subway y Shopify han incorporado la tecnología ledger, lo que hace que otras empresas la implementen también.

[298] Vid. https://www.meticulousresearch.com/product/blockchain-market/

5.1. Introducción

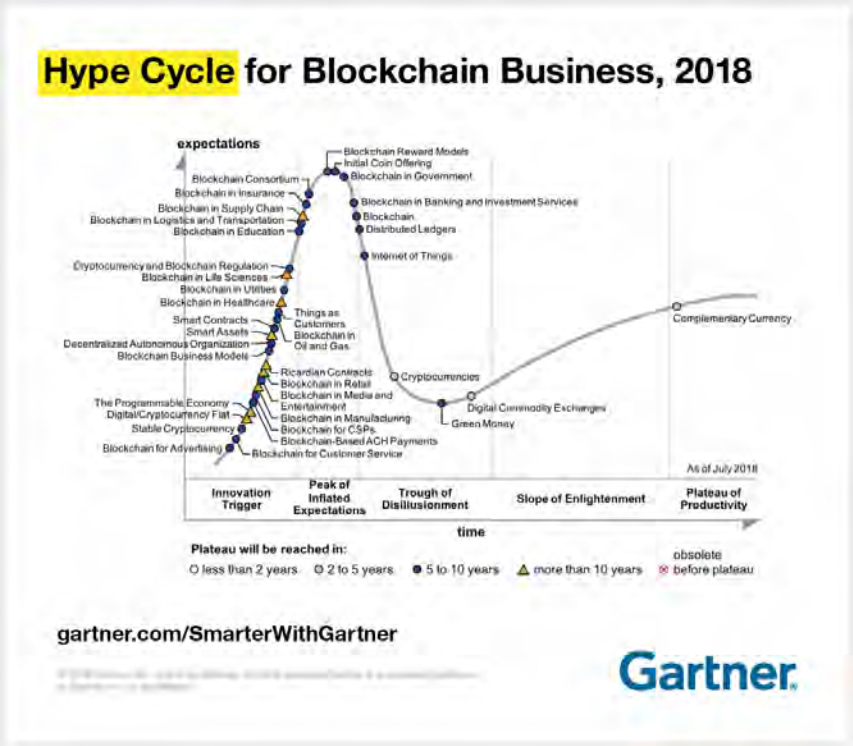


Imagen 33. Ciclo del bombo de Gartner para los negocios de Blockchain. Fuente: Gartner.

Como se puede ver blockchain en healthcare está por debajo que en blockchain de la educación, transportes, logística, aseguradoras, en el Ciclo de Gatner del "bombo" (ver gráfico superior). Eso significa que posiblemente para este 2019 ya estará cerca de la cima.

¿Por qué esta tecnología llega al sector de la Healthcare?

i. *El envejecimiento poblacional en los países desarrollados y las limitaciones presupuestarias*. Las nuevas iniciativas del sector se pueden centrar, según la empresa Capital Cell[299], en tres campos como son la introducción de datos médicos personalizados en *Blockchain*, la compartición de datos médicos con fines de investigación y desarrollo de nuevos fármacos, y la trazabilidad en la producción y el consumo de medicamentos. Actualmente, la sincronización entre sistemas depende de la intermediación de terceros actores de confianza.

ii. *Debido a la desconexión entre la sanidad pública y la privada*. Disponer de todos los datos médicos de forma pública, fiable y transparente a la vez que anonimizada, permitirá una mayor velocidad y un ahorro de costes en el Sector Público y Privado además de mayor eficiencia al producir mayores soluciones médicas disponibles para el usuario y consumidor. Dentro de poco, los pacientes en España dispondrán de aplicaciones donde los pacientes de hospitales públicos y privados podrán acceder mediante *Blockchain*, y permitirán compartir

[299]Ver https://www.consalud.es/saludigital/109/blockchain-pieza-clave-para-nuestra-salud_49823_102.html

la información con aseguradoras médicas para solicitar presupuestos de pólizas o con profesionales de salud u hospitales para ayudar en el diagnóstico o con farmacias o *startups de eHealth* para colaborar en estudios clínicos. Todo esto supondrá una auténtica revolución en el uso de los recursos médicos y su gestión.

iii. *Se espera que la seguridad de blockchain se extienda al intercambio de información*. Concretamente en cinco aspectos de la *eHealth*[300] ; la HCE de los pacientes; la información generada en ensayos clínicos; los datos genómicos; la información generada por los propios pacientes a través de dispositivos conectados y; los procesos de reclamación y pago de servicios sanitarios asegurados. El prime aspecto es clave. En concreto, el sistema de seguridad se trata de una base de datos compartida que funciona mediante *claves criptográficas* y se distribuye por diferentes bloques en los que es técnicamente *imposible modificar o borrar registros,* brindando una *auditoría estandarizada* y pauta "normas" formales para el acceso a los datos. Sólo se pueden añadir aportando transparencia y fiabilidad a la base de datos de salud.

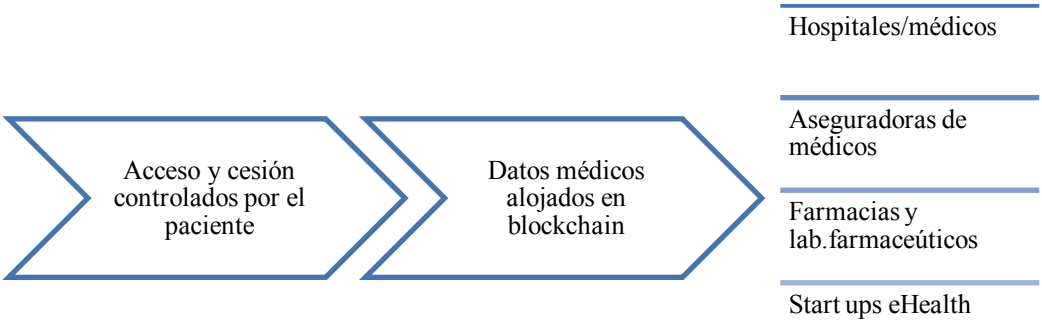


Imagen 34. Utilidades de la tecnología Blockchain en Salud.

Blockchain, por tanto, podría resolver el principal problema: la *seguridad e inviolabilidad de los datos* recogidos en sistemas integrales de recogida de información médica de usuarios. Además, permitirá compartir de forma segura información entre pacientes**,** lo que a su vez permitiría a los mismos compartir información con sus médicos o cuidadores.

5.1.1. Concepto

Un blockchain es esencialmente una infraestructura digital que agrupa registros de transacciones en bloques con sello de tiempo (de ahí el nombre). Estos son registrados por todos los participantes (nodos) de una red dada. Cada nuevo bloque hace referencia al anterior con hashes criptográficos, creando un registro inmutable de todas las

[300] Ver en http://curaesalud.com/wp-content/uploads/2017/09/Guia-Blockchain-para-el-sector-de-la-salud-Curaesalud.pdf

transacciones desde el primer bloque hasta el último. Las transacciones están certificadas para ser verdaderas, no porque una autoridad confiable (por ejemplo, un banco central, el gobierno, Facebook, etc.) valide la contabilidad centralmente, pero porque el ledger se distribuye en tiempo real a todos los participantes de la red. Un participante de la red no puede falsificar el registro, porque un algoritmo de consenso reconcilia la información a través de los nodos, detectando cualquier discrepancia. Esto significa que cada participante, es decir, paciente, sabe en todo momento lo que ha sucedido.

La tecnología blockchain permite que un paciente o consumidor de fármacos pueda identificarse en la Red sin tener que dar datos personales y a su vez donar o **monetizar** sus propios datos genómicos. Supone una auténtica revolución en los derechos individuales, comunicaciones y los negocios.

Es un registro de transacciones que permite crear un *libro de contabilidad digital* de datos y compartirlo entre una *red de participantes independientes*, al tiempo que emplea *encriptación* como una forma de validar que las entradas son correctas y no pueden ser cambiadas. *Blockchain* es una base de datos distribuida y apoyada en una red *peer to peer* (P2P) y, por tanto, compartida por múltiples nodos. Como consecuencia de este carácter distribuido no existe una autoridad central de control de la base de datos, lo cual es uno de los aspectos más importantes y poderosos de la tecnología *blockchain*. Las claves del Blockchain pueden ser los siguientes:

- *Cadena de bloques / Base de datos descentralizada*: La información no se almacena en una ubicación central. Los bloques se distribuyen y guardan en las máquinas de cada uno de los involucrados en la forma de bloques. Todas las blockchains han de actuar bajo las mismas reglas o protocolo para validar al bloque (y a la información recogida) y aportarla en la cadena de bloques. Una vez realizado, la cadena continua con la emisión del siguiente bloque, permaneciendo inalterable la información gracias a la criptografía. Cada bloque se conecta con los demás usando la lista vinculada, lo que hace que sea prácticamente imposible cambiar cualquier dato relacionado a una transacciónn finalizada.
- *Criptografía*: La nueva tecnología asegura los datos usando criptografía que no puede ser descifrada. Por tal entendemos un procedimiento que utilizando un algoritmo con clave (clave de cifrado) permite transformar un mensaje (sin atender a su significado) de forma que sea entendible de cara a personas que no tenga la clave secreta (clave de descifrado) del algoritmo empleado. Resulta además imprescindible para evitar manipulaciones, hurtos o introducciones de información en la cadena de bloques

- *Consenso (o una verdad):* Ssólo hay una verdad, y en el mundo de la tecnología blockchain, esta puede ser extraída usando algoritmos de consenso y establecida por cualquiera. Este consenso asegura la irreversibilidad de las mismas y debe proporcionar a todos los usuarios una copia inalterable y actualizada de las operaciones realizadas. El registro puede ser compartido y verificado por cualquiera que tenga acceso. Esta transparencia es la base para la confianza establecida.

Como establece Alex Preukschat[301], aunque generalmente hablamos de blockchain, la verdad es que no existe el concepto como tal (aislado) sino es acompañado siempre de un adjetivo, que modo que podemos diferenciar entre blockchain públicas, privadas o incluso híbridas.

5.1.2. Características de Blockchain/DLT

Las características y ventajas de aplicar la tecnología *Blockchain* podrían ser:

i. El acceso.

Los pacientes interactúan con multitud de proveedores de atención médica (pediatras, médicos, dentistas, etc.), y en cada momento, dejan datos dispersos en ubicaciones o jurisdicciones diferentes. *Blockchain* daría solución a la dificultad de acceder y rastrear los datos fragmentados. El contenido del registro médico[302] en bruto nunca se almacena en el *blockchain*, sino que se guarda de forma segura en la infraestructura de almacenamiento de datos existente de los proveedores. La mayor parte de casos de uso propuestos hasta la fecha están basados en *soluciones off-chain* o fuera de la cadena.

ii. La interoperabilidad.

[301] Preulschat, A. (2017). Blockchain: La revolución industrial de Internet, pp. 23. Edit. Gestión 2000.
[302] Por ejemplo, piénsese en el caso de *MedRec*[302] donde las transacciones en los bloques corresponden a cada una de las interacciones de la persona con un prestador de servicios o, en general, con un sistema reconocido y capaz de registrar datos de salud e incorporar al *blockchain* un enlace encriptado de acceso a los mismos con la correspondiente huella digital y sellado de tiempo. Por su parte, en *Embleema*[302], los proveedores, pacientes o investigadores que participan en DLT o *blockchain* privada sabrán a dónde se dirigen los datos, pero solo aquellos a los que se les otorga el derecho de verlos accederán a la información médica en sí, que aún estará protegida. Así, también en la *fundación suiza HIT,* su plataforma de *blockchain* permite distribuir el mercado como si se tratara de un mercado en línea (uber o Airbnb) pero sin autoridad central y sin monopolizar los datos de los individuos. Aquí, *blockchain* actúa como un control de acceso a toda la información de salud de una persona y ofrece una alternativa al problema de la interoperabilidad de datos de salud.

A veces todos los datos están en papel o en un formato estandarizado que no puede ser utilizado por otras aplicaciones[303]. Los problemas de interoperabilidad[304] son bastante frecuentes en el intercambio frecuente de datos, pero no sólo esto, también los pacientes se encuentran con dificultad a la hora de autorizar dicho intercambio. La solución estaría en un único interfaz y común donde los pacientes elijan lo que quiere compartir. Se podría recibir datos de diferentes puntos finales (centros médicos, servidores hospitalarios, ordenadores de pacientes en el hogar, etc.). Por ejemplo, durante una atención de urgencia en la que sea necesario consultar, por ejemplo, si está vacunado del tétanos o es alérgico a algún medicamento, el paciente podrá permitir que el centro médico haga la consulta a dichos dispositivos.

iii. La utilización de Smart contracts.

Los contratos inteligentes son un elemento fundamental puesto que establecen quiénes y cómo se van a producir las transacciones con una serie de clausulas incorporados en las cadenas de bloques garantizando su seguridad y proporcionando el entorno propicio para llevar a cabo su automático procesamiento. Por ejemplo, la blockchain pública de la *fundación suiza HIT*[305], permite al individuo acceder a sus datos bajo un contrato inteligente en el cual se utilizará el buscador de información sin necesidad de revelar identidades. No sólo los pacientes o usuarios podrán recibir fichas o tokens sino también los propios profesionales de salud. Todos los participantes se podrán repartir sus tokens con fines informativos pero también para servicios o bienes, como puede ser una oferta de bienestar o un descuento en el seguro social.

iv. El cifrado y la ciberseguridad.

Los ataques cibernéticos a los hospitales son una realidad en la actualidad[306]. Ahora bien, tanto el cifrado de datos como los procesos de validación hacen que *blockchain* pueda jugar un papel importante en la integridad de datos para los sistemas de

[303] PwC (2013). Kosten im Gesundheitswesen: Durch Digitalisierung über CHF 100 Mio. einsparen. Recuperado de https://www.swisscom.ch/de/about/medien/press-releases/2014/09/20140902-MM-KostenGesundheitswesen.html

[305] Vid. Scheuer, E. (2018). Whitepaper HIT Foundation Zug. Recuperado de https://hit.foundation/wp-content/uploads/whitepaper-hit-foundation-v2.pdf

[306] Independent (2017). *NHS cyber attack: Large-scale hack plunges hospitals across England into chaos.* Recuperado de http://www.independent.co.uk/news/uk/home-news/nhs-cyber-attack-hospitals-hack-englandemergency-patients-divert-shut-down-a7732816.html

tecnología sanitaria, y en la administración de los dispositivos médicos facilitando y haciendo más seguro el uso de IoHT.

v. La transparencia.

Cada vez es más frecuente que pacientes, investigadores, proveedores de atención sanitaria y organismos reguladores quieran compartir datos de una forma responsable,. Esto podría derivar en una economía de datos entre "consumidores" y "productores" de datos. Las aseguradoras y la industria farmacéutica entrarían en el juego gracias a *blockchain*. Pero, *¿la situación es igual para todas las blockchain?* La respuesta es negativa. En las redes públicas, en general, la transparencia es total puesto que cualquier usuario que se registre en la cadena es provisto de una copia de todo el blockchain, pudiendo ver en ella el estado actual de los activos y el historial de transacciones. En las redes privadas y federadas el acceso es restringido y mediante vía web para la mayoría de los usuarios.

vi. La autonomía y empoderamiento del paciente-consumidor. El valor de los tokens.

Los pacientes están cada vez más dispuestos, capaces y deseosos de administrar sus datos. El objetivo de blockchain es colocar al paciente en el centro de la gestión de sus atributos, pudiendo acceder, rectificar, actualizar, suprimir, recuperar sus datos y conceder permisos. Por ejemplo, la cadena de bloques de *Embleema* permite a los investigadores comprar tokens que les dan acceso a la información de salud que los pacientes comparten voluntariamente. Compensar a los pacientes de esta manera es realmente una forma de incentivar su participación en la investigación, a menudo por enfermedades en las que tiene sentido acelerar la investigación. Los proveedores también podrían ganar tokens al verificar la calidad de los datos.

Pensemos que el valor de un registro de salud[307] es de 13 dólares y un conjunto de datos de pacientes puede exceder de los 24.600 euros , donde la recopilación, estandarización y refinado -realizado por los intermediarios y los auditores- de los datos de los participantes y profesionales de salud tiene un coste. Es aquí donde tiene un papel muy importante Blockchain al facilitar la optimización del proceso y consultado por los pacientes reduciendo los costes transfiriendo los datos una vez verificadas las

[307] *Supra Cit.*

identidades. Por ejemplo, en el caso de investigación clínica, se podría conectar solo a los pacientes/usuarios directamente con aquellos que desean utilizar sus datos.

En este sentido, conviene destacar el papel responsable que conlleva la propiedad y el control de sus datos de soberanía para la adopción exitosa de nuevos servicios increíbles. Según MAAGHUL; "los nuevos tipos de ecosistemas enrollarán, desplazarán o disminuirán a los administradores de atención médica, los administradores de riesgos, los bancos y los intermediarios confiables de la cadena de suministro que atraerán a los consumidores y proveedores de los ecosistemas existentes hacia opciones de menor costo y quizás de generación de ingresos"

Por otro lado, en la Fundación suiza HIT, la tokenización de datos de salud permite a *todos los miembros* generar valor a partir de sus datos y pagar servicios de salud con *tokens*. Esta fundación es el primer ecosistema que permite a *todos* obtener compensación por la información de salud en lugar de pagar a otros para procesarla o almacenarla. Por tanto, también pueden generar valor el resto de los participantes, no solo los pacientes o usuarios de *eHealth*.

vii. La descentralización y la "no" necesidad de intermediarios.

Según TAMÉS[308], "Blockchain nos brinda la opción de desplazar a estos intermediarios y sustentar las garantías no en una entidad, sino en una comunidad, en un consorcio. Se apalanca en el concepto, por decirlo de alguna manera, del "círculo de confianza" un circulo, tan extenso (o público) como queramos, en el que todos los actores y participantes en el proceso velan por la integridad de éste. Se confirma que una transacción es viable porque todo el consorcio la ratifica y la registra en caso de ejecutarse". Los datos se almacenan localmente en bases de datos separados de los pacientes y proveedores. Solo hay copias de datos en cada nodo de la red. Pensemos el consorcio de universidad investigadora con empresa tecnológica y los miembros de una asociación de enfermos, quienes a cambio de una contraprestación transmiten su información personal de salud (biomarcadores, genética, etc.). Estas instituciones podrían tener su propio nodo provisto solo con permisos para ver *información concreta* sobre su salud que tienen que verificar (sin poder conocer en ningún momento el precio

[308] Tamés, A. (2018). Blockchain: La disrupción del rol del paciente en el ámbito de la salud. *Revista Sociedad Española de Informática de la Salud*. Pág. 8. Recuperado de https://seis.es/wp-content/uploads/2018/04/128.pdf.

acordado por la información). Al finalizar satisfactoriamente el proceso establecido en el *Smart Contract*, el dinero se transferiría automáticamente al paciente.

5.2. Clasificación de Blockchain

i. Blockchain pública.

La autoridad francesa de protección de datos (CNIL), señaló en su reciente informe que "las Blockchains públicas son accesibles para cualquier persona en el mundo. Cualquiera puede realizar una transacción, participar en el proceso de validación de bloque u obtener una copia de blockchain. Los bloques tienen reglas que definen quién puede participar en el proceso de aprobación o incluso realizar transacciones. Según el caso, pueden ser accesibles a todos o ser de acceso limitado"[309]. Además, pueden ser permisionadas o no permisionadas. Por ejemplo, el consorcio español de blockchain *Alastria* es una *Red pública permisionada*. En cambio, por ejemplo, la Red de blockchain Bitcoin es pública no permisionada ya que cualquiera puede ser un nodo y unirse a la red, y convertirse en un minero para servir la red y buscar una recompensa.
¿Y cómo funciona? Según ALLENDE, en general, "el procedimiento para participar es descargarse la aplicación correspondiente y conectarse, de forma automática, con un determinado número de nodos a los que se les pregunta por la versión más actualizada de la cadena. Una vez el nodo está actualizado, tiene los mismos derechos y deberes que el resto de participantes a la hora de proponer y validar transacciones, replicar las transacciones que escucha o minar -si desea hacerlo-. También en su mayoría, la seguridad de estas redes está basada en protocolos de consenso y funciones hash, y los usuarios interactúan con la red de forma anónima" [310].Por tanto, son aquellas a las que tiene acceso *cualquier persona*[311] y tiene funciones como ayudar a encontrar más nodos que pueden verificar la cadena; y minimizar la confianza necesaria en los sellos de

[309] Ver en https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data
[310] Allende López, M. Blockchain: cómo desarrollar confianza en entornos complejos para generar valor de impacto social. *Banco Interamericano de Desarrollo*. Recuperado de https://webimages.iadb.org/publications/spanish/document/Blockchain-C%C3%B3mo-desarrollar-confianza-en-entornos-complejos-para-generar-valor-de-impacto-social.pdf
[311] Concretamente, para PREUKSCHAT, "una red pública es una red descentralizada de ordenadores que utilizan un protocolo común asumido por todos los usuarios y que permite a éstos registrar transacciones en el libro mayor (ledger) de la base de datos. Esas anotaciones son inalterables, si bien los participantes en una blockchain de estas características pueden verificar de forma independiente y por consenso de los cambios que se realizan en los registros".

tiempo de los mensajes. Como veremos será la blockchain con más controversia jurídica ya que cualquiera puede unirse sin permiso y no es posible asegurar que los participantes estén de acuerdo con los términos y condiciones contractuales, de hecho, antes de ingresar, ni es posible conocer la ubicación geográfica de los miembros, ni evaluar la custodia de sus datos o el cumplimiento de RGPD y otras regulaciones. Esto implicaría que de primeras no serían compatibles con la normativa europea.

ii. Blockchain privadas.

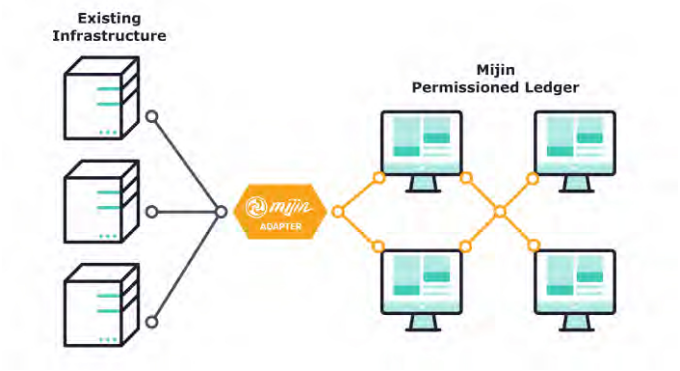
Para el CNIL, "las Blockchains privadas[312] están bajo el control de un actor que solo controla la participación y la validación. Según algunos expertos, estos usos no respetan las propiedades clásicas de esta tecnología, incluida la descentralización y la validación distribuida. En cualquier caso, no plantean una cuestión particular de conformidad con el RGPD, son simples bases de datos distribuidas clásicas".

Por el contrario, para participar de una red de blockchain privada[313], se requiere una *invitación* y ésta puede ser validada personalmente por quien inicia la red o por un ciertas reglas que éste deja preestablecidas. Esto podría interesar a organizaciones las empresas que quieren tener una red de Blockchain distribuida internamente o con sus proveedores y ciertas contrapartes. Hay varias formas en que se puede controlar esta red interna, por ejemplo, a través de los participantes existentes o bien de una autoridad reguladora que otorgara licencias para participar (terceros de confianza). Puede funcionar como si se tratara de una "plataformas de gestión empresarial" que conecta a diferentes departamentos y sistemas dentro de una empresa, grupos empresariales o incluso, consorcios. Así por ejemplo, *Hyperledger* o *Nem* son ejemplos de redes

[312] Para PREUKSCHAT, Las *blockchain* privadas, en todo caso son: (i) "*Privadas*, porque no todos los datos inscritos en la blockchain tienen difusión pública y solo los participantes o usuarios pueden acceder y consultar todas o algunas de las transacciones realizadas; (ii) *Cerradas*, porque solo las personas o entidades invitadas a participar adquieren la condición de usuarios o registradores de las transacciones. En este sentido, el protocolo predeterminado podrá incluir distintos niveles de acceso a los usuarios, de modo que unos puedan tener la capacidad de registrar información y otros tener vetada esta opción; (iii) *Anónimas,* ya que una blockchain privada puede establecer el nivel de anonimato que quiera para realizar o proteger transacciones. Los usuarios que registran anotaciones pueden estar o no perfectamente identificados; (iv) *Distribuidas*, porque el número de nodos de los que se componga la blockchain privada puede estar limitado al número de participantes o a cierto número de ellos. En cualquier caso, todos los nodos se conocen. A mayor número de nodos operativos, menos es la posibilidad de sufrir ataques. En la privada, los participantes se comprometen en mantener la estabilidad del sistema".

[313] Para MAAGHUL, "la implementación exitosa en el futuro de este tipo de solución es muy específica para cada caso de uso y apesta con la centralización oculta (y el riesgo tradicional) y, a veces, se da como una solución que busca un problema" . Recuperado de https://www.pointnurse.com/blog/do-you-have-a-healthcare-blockchain-strategy/

privadas desarrolladas más conocidas que pueden ser implantadas por los usuarios de esta tecnología.



Fuente: Nem.io. Blockchain privada

Al final las blockchain privadas sacaban siendo conocidas en el mercado como las *"Distributed Ledger Technology"* (profundicemos algo más adelante).

iii. Las Blockchain híbridas.

Son una combinación de las públicas y privadas donde los nodos participantes son invitados pero todas las transacciones son públicas. Un ejemplo de blockchain híbrida desarrollada es *Evernym* para la SII (sistemas de identificación digital soberana, de la que hablaremos en los próximos capítulos). [314]

Dicho lo anterior, sería interesante analizar las redes *blockchain ("desarrolladas")* más conocidas para *desarrollar* una aplicación descentralizada (aplicadas a nuestra temática y casuística, principalmente):

i. *Ethereum* (para Blockchain pública)

Aquí cualquier persona puede desarrollar una aplicación descentralizada. Por ejemplo, si un usuario quisiera crear una aplicación de "smart contract" [315] por sí solo sería muy

[314] Al margen de ello, también pueden ser clasificadas mediante *generaciones*[314], teniendo en cuenta sus funcionalidades: (i) *Primera generación* en la que surge primera red *Blockchain*, "*Bitcoin"*. La idea principal consistía en la creación de un sistema distribuido y descentralizado que se utilizara como un almacén de registros "transparente" a todos los participantes en la red; (ii) *Segunda generación* toma como base la generación anterior e introduce un nuevo elemento en la red con el que interactuar, las "*criptomonedas"*. Están totalmente orientadas al mundo financiero, en concreto a la funcionalidad de poder hacer transacciones monetarias entre dos entidades; (iii) *Tercera generación* en el que aparecen los "*smart contracts"* o contratos inteligentes, la base para la creación de aplicaciones descentralizadas. Este tipo de contratos son autoejecutables y están almacenados en la red Blockchain , por lo tanto, todo el mundo puede confiar.

[315] Es más, incluso, la tecnología IoT se puede "aliar" con la red *blockchain Ethereum*, es el caso de *Slock.it* que lanzó una estación autónoma de carga para vehículos eléctricos, que integra un contrato

difícil ya que tendría que desarrollar su propia red de Blockchain y luego invitar a más usuarios a participar como verificadores. El beneficio de Ethereum es que, a cambio de una contraprestación el usuario puede aprovechar la red pública ya desarrollada.

ii. *Hyperledger* (para Blockchain privada).

"Es un proyecto de código abierto nacido en diciembre de 2015 y albergado en la Fundación Linux que nació con el objetivo de crear un ecosistema centrado en crear soluciones de código abierto en el ámbito corporativo con DLTs y en la práctica por ahora se está centrando en el desarrollo de tecnología blockchain privada para corporaciones" (NIETO). Son miembros algunos de los gigantes tecnológicos como Cisco, IBM, Intel, SAP, y también startups que deciden donar su proyecto a Hyperledger para ganar visibilidad y generar una comunidad alrededor de su código como por ejemplo, Sovrin (compañía estadounidense referente en sistemas SSI de identificación soberana) con Hyperledger Indy"[316][317]. La experta Nieto ha diseñado un tutorial accesible explicando la programación de cómo se hace una red privada con Hyperledger[318].

5.3. Aplicabilidad a la Atención Sanitaria: utilidades y casos reales.

A continuación se señalan posibles casos de utilización de la tecnología blockchain en salud:

---

inteligente que usa esta tecnología. En nuestro caso y siguiendo nuestra temática central, podemos trasponer este ejemplo al sector de la salud. Recordemos el caso del cepillo de dientes inteligente del que hablábamos en la presentación.

[316] Ver en https://www.eleconomista.es/economia/noticias/8899454/01/18/Hyperledger-la-Blockchain-privada-que-todos-tenemos-que-conocer.html

[317] Nieto Galán, M.T. (2017). *Health: Registro médico electrónico en una red Blockhain.* (Trabajo fin de máster, Universidad Carlos III). Recuperado de https://e-archivo.uc3m.es/bitstream/handle/10016/26274/TFG_Maria-Teresa_Nieto_Galan.pdf?sequence=1&isAllowed=y. (La autora señala que está compuesta por tres componentes principales (i) "Servicio de identidad de Hyperledger. El servicio controla las identidades de todos los participantes: organizaciones, validadores, transacciones, los objetos incluidos en las transacciones -activos y contratos inteligentes-, y compontes del sistema de como redes, servidores, entornos de ejecución. Los validadores, durante la configuración de red, pueden determinar el nivel de permiso que se requiere para realizar transacciones; (ii) Blockchain de Hyperledger. Consiste en tres componentes principales: el protocolo peer-to-peer", el "distributed ledger" -la contabilidad distribuida-, y el "consensus manager" -gestor de consenso-; (iii) Contratos inteligentes de Hyperledger. Los cuales tienen distintas políticas de acceso. En primer lugar, la pública, utilizados por las transacciones públicas donde cualquier miembro de la red lo puede invocar. En segundo lugar, la confidencial, desplegado por transacciones confidenciales que solo pueden ser usados por miembros validadores. Y por último, la de acceso controlado, desplegado por transacciones confidenciales que utilizan los token de la transacción para identificar a los invocadores").

[318] Vid. https://medium.com/@_mtnieto/creando-una-red-privada-blockchain-con-hyperledger-fabric-2e1567167325

i. *Poseer y compartir datos médicos.* Los pacientes y usuarios de *eHealth* pueden compartir su historial médico (HCE) completo de forma anónima con investigadores y organizaciones de atención médica

ii. *Ensayos clínicos y gestión de consentimiento.* Los investigadores tienen acceso a cantidades más grandes de datos más confiables ayudando a los estudios clínicos.

iii. *Micropagos o pequeñas recompensas otorgadas a los pacientes* por apegarse a sus planes de atención médica cada vez están más extendidos. Los pacientes podrían recibirlos cuando las grandes compañías farmacéuticas realizan análisis sobre sus datos. Pongamos un ejemplo, si un paciente afirma haber realizado una prueba de escáner médico, el "propio escáner" así como un médico, tienen que validar esa transacción en *blockchain*. Sólo si *todas* las partes están de acuerdo, se añade ese hecho al registro, desencadenándose acto seguido el pago de los gastos pertinentes.

iv. *Integridad de la cadena de suministro y seguridad de datos.* Las compañías de atención médica podrían registrar información importante sobre los productos, como los efectos secundarios de un determinado medicamento. El uso de un blockchain significa que deben hacerse menos copias de los ledgers de información dentro de la compañía, y que aquellos que existen tienen un riesgo mucho menor de ser presa de ciberataques. Los datos personales y SSN de los niños se venden en la Web oscura incluyen nombres, números de teléfono, direcciones y números de Seguro Social[319].

v. *Prevención del fraude.* Por su naturaleza proporciona una forma segura de confirmar las reclamaciones de seguro o identificar las falsas reclamaciones. La información sobre prescripciones de medicamentos, visitas a instituciones médicas o contratos de un paciente se puede verificar con precisión en cualquier momento.

vi. *El uso de la criptomoneda.* Las empresas de otras industrias han comenzado a aceptar la criptomoneda como forma de pago factible. Por ejemplo, *Teledactyl,* lo realiza. No obstante, queda por ver si la criptomoneda se convertirá en un método de pago tan significativo en la atención médica como en otras industrias.

[319] https://retina.elpais.com/retina/2018/12/21/innovacion/1545388739_968425.html?Id_externo_rsoc=TW_CM_RT_bc_phm

En todo caso parece que este cambio podría venir de la mano de la industria del seguro de salud.

Ahora bien, *¿cómo se materializan en proyectos reales de blockchain? ¿quién apuesta por las iniciativas y su implantación? ¿los gobiernos, las tecnológicas o ambos? ¿qué países toman la posición de lideres internacionales?*

Estonia o los países de los *Emiratos Árabes* son lugares donde se apuesta fuertemente por la implantación de blockchain en el cuidado de la salud. Estonia, concretamente, es un país "en la nube" y las bases de datos de los registros con información ciudadana y la tarjeta digital de identificación se apoyan en blockchain. En el caso del sistema sanitario mientras los registros de eHealth se encuentran en las tradicionales bases de datos asistenciales a las que se puede acceder desde el portal del paciente, el uso de blockchain realiza el servicio de firma verificable. De esta forma la *Estonian eHealth* Foundation está asegurando los registros médicos de más de 1 millón de pacientes. El sistema es totalmente transparente y cualquier paciente puede iniciar sesión y ver exactamente quién ha estado viendo sus registros e incluso puede restringir el acceso a grupos de usuarios.

De igual forma el gobierno de *Dubái* también ha lanzado un proyecto para establecer una plataforma blockchain con tres finalidades; el ahorro en transacciones administrativas, el fortalecimiento de una industria multisectorial de negocios que usen la plataforma y el liderazgo internacional.

Como vemos el papel de los gobiernos nacionales es fundamental. No obstante, es frecuente la aparición de alianzas entre gobiernos y compañías tecnológicas puesto que es el gobierno quien apuesta principalmente por preservar la salud de la ciudadanía. Algunos ejemplos son:

- La alianza entre la *Administración de Alimentos y Medicamentos de Estados Unidos* **(**FDA**)** e *IBM Watson Health* para explorar el uso de *Blockchain* en el uso compartido de información médica. El convenio incluye el intercambio de datos de pacientes procedente varias fuentes, incluyendo registros médicos electrónicos, ensayos clínicos, datos genómicos y datos de salud procedentes de dispositivos móviles, wearables e IoT
- La alianza entre *Alibaba Health Information Technology* y el Gobierno Chino Hospitales, clínicas, organizaciones gubernamentales y demás organizaciones del sistema deben estar dispuestos a colaborar para crear, prototipar y probar los conceptos fundamentales que harán las

bases para las historias clínicas del futuro[320]. El *sistema de blockchain* cada vez que se pide un análisis de sangre, médico y paciente tienen su identificador único. La orden del análisis, los participantes y la fecha y hora serían guardados como un bloque más en la cadena de ese paciente en particular.

Pero para entrar en más detalle, el *Becker's Hospital*[321] enumera entre otros los siguientes ejemplos de proyectos:

- *Accenture* (Irlanda, Europa). Accenture se asoció con Microsoft y Avanade para desarrollar un prototipo de identidad basado en tecnología de cadena de bloques que podría proporcionar una identidad digital para 1.100 millones de personas que no tienen una identificación formal.
- *Astr*i (Instituto de investigación de ciencia y tecnología, Hong Kong, China). Astri desarrolló una plataforma de tecnología de la salud que apunta a impulsar las interrupciones en el campo de la atención médica tradicional con monitoreo preventivo de la salud, computación médica y diagnósticos.

- *Bloq* (EEUU). La solución de software bloqEnterprise de la compañía permite a los usuarios crear, probar, actualizar y personalizar las cadenas de bloques permitidas.

- *Brontech* (Australia). La compañía distribuye el almacenamiento de datos y asegura la integridad al tiempo que recompensa a los usuarios con una moneda digital nativa administrada en la cadena de bloques, efectivo u ofertas de socios comerciales.

- *BurstIQ* (EEUU.). La plataforma LifeGraph reúne los datos de salud de un individuo en un solo lugar y permite a los usuarios administrar datos a través de contratos inteligentes. *BurstChain* es la plataforma de la cadena de bloques de datos grandes de la compañía para administrar de forma segura conjuntos de datos de salud grandes y complejos.

- *Factom* (Austin, Texas, EEUU). Factom es una empresa de tecnología blockchain-as-a-service que recibió $ 8 millones en fondos de la Serie A en abril de 2017.

- *HealthCombix* (EEUU). La plataforma de HealthCombix es una red de gestión de riesgos y pagos de atención médica basada en token que permite pagos, monetización de activos de datos y ajuste de riesgos.

[320] Recuperado de http://ehealthreporter.com/es/noticia/blockchain-una-tecnologia-que-revolucionara-la-salud/
[321] Ver en: https://www.beckershospitalreview.com/lists/25-blockchain-companies-in-healthcare-to-know-2017.html

- *Health Linkages* (EEUU). Permite a las instituciones de salud realizar análisis de datos mejores, más seguros y más privados en salud de la población y medicina de precisión. Health Linkages recopila y cifra los datos cuando se crean y mantiene un historial completo de los datos y sus vínculos durante toda la vida útil del punto de datos.

- *IBM Blockchain Bluemix* (EEUU). IBM Blockchain es el primer servicio administrado para Hyperledger Fabric, que permite la creación de redes empresariales de blockchain que los propietarios pueden controlar y distribuir en diferentes organizaciones.

- *Medicalchain* (Reino Unido, Europa). Utiliza la tecnología blockchain para almacenar los registros de salud de manera segura, de modo que los médicos, hospitales, laboratorios, farmacéuticos y aseguradores de salud pueden solicitar el permiso de un paciente para acceder al registro, así como registrar las transacciones en el libro mayor distribuido.

- *MedRec* (EEUU). Investigadores de estudiantes graduados en el Instituto de Tecnología de Massachusetts en Boston desarrollaron MedRec, un sistema para administrar registros médicos utilizando Ethereum, una plataforma descentralizada para aplicaciones. MedRec está diseñado para que los pacientes controlen sus datos médicos, incluidos los registros clínicos de EHR y los datos de dispositivos de salud personal como Fitbit. Los pacientes pueden permitir que los proveedores de atención médica, investigadores y familiares accedan de forma segura a sus datos. Los investigadores médicos también pueden extraer los datos para mantener el registro de autenticación de blockchain y recibir a cambio metadatos médicos anónimos.

- *Netki* (EEUU). Netki lanzó un servicio de identidad digital para hacer que blockchain sea seguro para aplicaciones de negocios, finanzas y atención médica.

- *Patientorty* (EEUU). permite a los usuarios crear perfiles en una aplicación móvil para almacenar, administrar y compartir información médica de forma segura. La solución es compatible con Epic, Cerner, Allscripts y Meditech, entre otros sistemas de EHR.

- *PointNurse* (EEUU) Fundada en 2014, es una plataforma de atención virtual y bajo demanda que permite a las enfermeras dirigir la atención centrada en el consumidor fuera del ámbito hospitalario y clínico. La plataforma permite a los profesionales con licencia participar en conversaciones seguras y privadas con pacientes

- *PokitDok* (EEUU). Proporciona una plataforma de desarrollo de software segura y gratuita para empresas de atención médica. La compañía impulsa DokChain, una red distribuida de procesadores de transacciones que operan con datos clínicos y financieros en toda la industria de la salud. Hasta marzo de 2017, la compañía había recaudado $ 48 millones para desarrollar DokChain.

- *ScalaMed* (Sydney, Australia). Proporcionar una aplicación descentralizada para pacientes, médicos y farmacéuticos para administrar, prescribir y dispensar medicamentos recetados.

- *Stratum* (Irlanda). La tecnología de prueba de procesos de la compañía permite la trazabilidad y la transparencia de los datos, y crea una pista de auditoría común asegurada por blockchain y criptografía.

- *Tierion* (Hartford, Conn.). HashAPI de Tierion permite a los desarrolladores anclar hasta 100 registros por segundo en la cadena de bloques de forma gratuita, con sello de tiempo y seguridad de datos. Tierion fue la primera compañía en unirse a Blockchain Lab de Philips para explorar el uso de blockchain en la atención médica.

- *YouBase* (Englewood, Colorado). YouBase combina tecnologías compatibles con blockchain para ofrecer un contenedor seguro y flexible para datos independientes. Está diseñado para descentralizar información sensible del consumidor y personal al compilar una única fuente de datos anónimos.

5.4. Aplicabilidad a la Industria Farmacautica: utilidades y casos reales.

A señalar unos datos muy importantes para entender la relevancia de la cuestión; el mercado anual de desarrollo de medicamentos es de 140 mil millones dólares y las compañías farmacéuticas están comprando conjuntos de datos costosos, como lo demuestran los acuerdos recientes. Por ejemplo, *Vertex* paga 10,000 dólares por paciente por año a la Fundación de Fibrosis Quística. *Roche* compró *Flatiron*, valorando los registros de pacientes con cáncer en aproximadamente 9,500 dólares al año. El problema es que los métodos actuales de recolección de pruebas de ensayos clínicos son costosos, lentos e ineficientes. El coste de los ensayos por paciente es de 36,500 dólares en promedio. Los pacientes no reciben compensación cuando se venden sus datos agregados y no dan su consentimiento explícito. Finalmente, los datos agregados no tienen la calidad de los datos individuales a nivel del paciente que se requieren normalmente. Por lo que esta tecnología traería beneficios al permitir a las personas que deseen participar en los ensayos agreguen los datos asociados con su salud y hacerlos visibles para todos los reclutadores asociados con las empresas farmacéuticas. De este modo, los reclutadores podrían seleccionar a la persona en base a la información de sus registros y a este último le llegará una notificación, la cual, si es aceptada, revelará al reclutador los datos de identificación del participante para que este sea

contactado. Los fabricantes de medicamentos que llevan a cabo ensayos clínicos podrían compartir datos clínicos y muestras médicas de forma más segura y sencilla. Incluso, esta tecnología podría tener un papel importante para proteger los datos delicados de la industria de ataques cibernéticos. La tecnología permite el intercambio de datos seguro, eficiente e interoperable. La integridad de la información es asegurada por la validación criptográfica de cada una de las transacciones que se llevan a cabo. Esto es importante para garantizar la transparencia de la restricción de datos y evitar las falsificaciones, invenciones y el "embellecimiento" de datos.

Las empresas tecnológicas comienzan a interesarse y firman alianzas con empresas de la *big pharma* como por ejemplo:

- *Sanofi y Alphabet*. Crean la joint venture Onduo, como una clínica virtual contra la diabetes
- *Microsoft y Novartis* Desarrollar dispositivos que se utilicen frente a las enfermedades crónica
- *HP y Johnson & Johnson***.** Tecnología de impresión 3D aplicada a la salud
- *Pfizer y IBM* Watson. Investigación en inmunoncología.
- *Alibaba y GSK*. Ayuda médica online sobre la vacuna frente al papiloma humano.

La mayor parte de las alianzas entre laboratorios y tecnológicas están en el campo de diabetes, seguido de respiratorio , oncología, neurología o cardiovascular. Ahora bien, existen iniciativas donde atención médica e industria farmacéutica actúan conjuntamente en el marco de grupos o consorcios como en las siguientes:

- *Health Co.* que trata de establecer una relación directa entre pacientes e investigadores.
- *Zenome* es una hay plataforma de blockchain que permite monetizar los datos genómicos[322]. El valor de mercado de los datos genéticos alcanzó los $ 5.9 mil millones de dólares en 2010, una cifra que se prevé que crecerá significativamente en los próximos años[323].
- *Doc.Ai* (Palo Alto, California, EEUU). La plataforma Robo-Genomics de Doc.AI es un agente conversacional profundo diseñado para mejorar la comprensión de datos genéticos y brindar apoyo en la toma de decisiones. El agente puede conversar sobre enfermedades, rasgos, farmacogenómica y planificación familiar. El fundador de Doc.Ai, Walter De Brouwer, fue uno de los tres partidos que ejecutaron el primer contrato de seguro de vida en la cadena de bloques pública con bitcoin en enero de 2017.
- *Salud Wizz (*EEUU). La compañía combinada está trabajando en Mercatus, una plataforma que permite a las personas crear su propia cartera de salud digital y otorgar acceso a investigadores

[322]Ver en: https://zenome.io/
[323] Jones, B. (13 de septiembre de 2017). 23 andMe is Raising 200 millones de dólares al hacer medicamentos desde tu ADN. *Futurism*. Recuperado de https://futurism.com/23andme-is-raising-200-million-to-make-drugs-from-your-dna/

médicos, científicos de datos de salud, compañías farmacéuticas y otros en un solo mercado para avanzar en la medicina de precisión. Mercatus permitiría a los usuarios escribir contratos inteligentes en la cadena de bloques Ethereum para intercambiar datos de salud por cripto-moneda.

- *Bloque MD* (Tailandia). Es una plataforma que permite una interoperabilidad segura y de alta integridad de datos en hospitales, nuevas empresas de tecnología de la salud, laboratorios, seguros, reguladores y, definitivamente, pacientes a través de estándares de datos y API bien definidos.

A modo de conclusión y para cerrar este apartado recalcaremos la importancia de la privacidad. En el informe anteriormente señalado de *McKinsey* se señalaba algo alarmante pero que no nos puede extrañar:

> "Para desarrollar las combinaciones más prometedoras de manera eficiente, estas compañías farmacéuticas necesitan acceder y compartir los primeros datos y mejorar su infraestructura digital para administrar ensayos complejos y presentaciones en forma conjunta. Múltiples "terceros" están agregando datos de salud y poniéndolos a disposición de proveedores y pagadores."[324]

5.5. Aplicabilidad en Industria Aseguradora: utilidades y casos reales.

Hay varias utildades y casos reales posibles. A continuación señalamos las más importantes siguiendo el listado de "aplicaciones prácticas" del artículo que publicó acertadamente la *Community of Insaurence* (2018)[325] como referencia:

i. Facilitar *la gestión de la información y las transacciones entre los diferentes stakeholders o participantes* (pacientes, médicos, hospitales y aseguradoras) mediante la tokenización de archivos, registros médicos y acuerdos, lo cual conllevará una eficiencia de los procesos de negocio. Un ejemplo es la implantación del proyecto en la Fundación suiza HIT . Por tanto, esto se traducirá en más facilidad para una *relación dinámica entre aseguradora / cliente*. Y es que como decíamos en el capítulo 1; "La digitalización ha llegado tan fuerte a esta industria que aseguradoras tan grandes como la americana *La John Hancock* dejará de suscribir el seguro de vida tradicional y solo trabajará con *pólizas interactivas*. La novedad más importante es la obligatoriedad de que el cliente se someta a un seguimiento de la condición física y los datos de salud a través de dispositivos wearables, como pulseras de actividad y relojes inteligentes o smartphones. Con esta situación, los asegurados tendrán descuentos por alcanzar objetivos de ejercicio físico quedándose registrados sus datos de salud en los dispositivos *Fitbit o Apple Watch*

[324] Es de señalar en este punto, que la conocida Farmaindustria está trabajando en el desarrollo de un nuevo código de conducta de protección de datos personales en el ámbito de la investigación clínica y de la farmacovigilancia**.** Los objetivos del este código entre otros son uniformizar criterios en la recogida de datos, la obtención del consentimiento y el proceso para pseudonimizar los datos.

[325] Vid. https://communityofinsurance.es/blog/2018/02/25/blockchain-y-seguro/#1519579978160-bb60bc98-c05c

y pueden obtener tarjetas regalo, descuentos en su póliza y otras ventajas registrando sus entrenamientos diarios. Este nuevo escenario ha creado revuelo y debate en el sector de la privacidad planteando cuestiones como si las aseguradoras están legitimadas para usar datos y así, *seleccionar a los clientes más rentables*, mientras aumentan los cobros a aquellos que no participan de los programas de actividad física". En España ha llegado también el uso de apps de aseguradoras que puede reportar beneficios para el asegurado.

Imagen 35. Descuentos por utilizar dispositivos. Fuente: Vivaz. Línea Directa [326]

ii. Permitir *la tokenización de los atributos de los registros médicos* favoreciendo la creación del historial clínico y una visión única de información para los pacientes. Tiene clientes que son aseguradoras por tanto como clientes son responsables del tratamiento y los encargados son esta empresa proveedora blockchain que subcontratará a otras organizaciones. Por ejemplo, Bodyo, trata de un sistema que utiliza se trata de IoT, IA y Blockchain con "body health utility token". Cuentan con un contrato inteligente entre un sistema de recompensa para los pacientes que muestran un buen comportamiento.

Imagen 31. Bodyo. Fuente Bodyo

iii. *Posibilitar registros de salud integrales e interoperables.* Posibilitará una *mayor seguridad* y capacidad para establecer la confianza entre las entidades.

iv. *Respaldar tareas administrativos y estratégicas con contratos inteligentes*[327]. Blockchain podría recopilar automáticamente registros de acuerdos, transacciones y otros conjuntos de información

[326] Vid. https://www.vivaz.com/app/actividad.html

[327] "A modo de ejemplo, imaginemos que introducimos un contrato inteligente asociado a un seguro incendio de vivienda. Esto implicaría agregar al blockchain una transacción que implica la transferencia del monto acordado al beneficiario y condicionar la transferencia a que se cumplan ciertas condiciones como ser que la alarma de incendio se haya disparado, que Bomberos haya publicado un reporte de incendio con ciertas características (ej.: domicilio del asegurado, que haya sido accidental, etc.) y que se cumplan condiciones formales (ej.: póliza vigente). Los participantes del blockchain (ej.: una o varias aseguradoras, corredores, beneficiarios) *podrán verificar en tiempo real el cumplimiento de las condiciones del contrato inteligente*, y una vez que la red acuerde que las condiciones del contrato están cumplidas, *automáticamente ejecutarán la transacción acreditando el monto acordado al beneficiario"*. Recuperado de https://www2.deloitte.com/uy/es/pages/strategy-operations/articles/La-transformacion-de-las-companias-de-seguros-en-la-era-digital.html

valiosa, luego unir la información y actuar sobre los datos mediante contratos inteligentes[328]. También se puede m*ejorar la precisión del directorio de proveedores*. Esta es una cuestión importante para determinar y perfilar las posiciones jurídicas en materia de protección de datos y enlazar las relaciones jurídicas con cierta formalidad.

v. *Detener el fraude de manera más efectiva* Cuando se envía información fraudulenta a una aseguradora de vida o de salud a través de reclamos falsos, aplicaciones falsificadas u otros canales, los *contratos inteligentes pueden ayudar a determinar si la presentación es válida*. La definición de fraude en seguros es: "Toda acción u omisión por parte de los intervinientes en la contratación de un seguro o declaración de siniestro, tendente a obtener ilegítimamente un beneficio propio o para favorecer a un tercero". Hemos de partir de la base que la relación del asegurado con la entidad aseguradora está basada en la mutua confianza, y no siempre se da. Respecto a la jurisprudencia actual relacionada con la selección de riesgo, es interesante comentar que ha habido varias sentencias donde los tribunales han dado la razón a las Compañías, en casos donde el asegurado había falseado el cuestionario de salud. Por poner un ejemplo, la Audiencia Provincial de Alicante, el 13 de noviembre del 2007[329], estimó el recurso interpuesto por la Compañía de Seguros ASISA, revocando la sentencia de instancia al haberse acreditado que la asegurada omitió ciertas patologías en la cumplimentación del cuestionario previo sobre salud, lo que exime a la aseguradora de la reclamación planteada.

5.6. Fases del proyecto blockchain aplicado al cuidado de la salud.

Inicialmente, antes de profundizar de lleno, convendría señalar el *tipo o perfil de blockchain* que se utilizaría como estándar para el análisis jurídico que se realizará en la segunda parte del presente trabajo. Teniendo en cuenta el escenario real y la implantación real de estas plataformas en entidades líderes europeas y teniendo en cuenta el gran abanico de utilidades que puede ofrecer. Es por ello, que se optaría por inclinarse por una *blockchain descentralizada o DLT permisionada* donde cualquiera pudiera acceder cumpliendo una serie de requisitos. Hay que tener en cuenta que los nodos serán entidades o instituciones conocidas (o de confianza) que "otorgarán su sello de validez" para aceptar nuevos miembros o participantes a esa Red. Se podría contratar servicios de una plataforma que desarrollara el proyecto (por ejemplo, a la citada

[328] De hecho, se pueden incorporar *pólizas como un contrato inteligente*. Es decir, las condiciones de ejecución de una póliza en forma de un pequeño programa y se definen actores externos que proporcionarán la información para determinar el cumplimiento de las condiciones del contrato inteligente.

[329] Vid. STC Audiencia Provincial de Alicante, sec. 8ª, S 13-11-2007, nº 423/2007, rec. 342/2007. Pte: García-Chamón Cervera, Enrique.

NEM[330] (ver capitulo 2.3) orientada a la creación de nuevos activos digitales y elaboración de *smart contracts*).

Dicho lo anterior, procedamos a desarrollar un posible esquema de implantación de *blockchain* de cuidado de la salud teniendo en cuenta las siguientes cuestiones:

i. El cumplimiento de las 5 fases.

En primer lugar, será conveniente definir el problema a resolver u objetivo a alcanzar (como dijimos al inicio del trabajo) en el ámbito del cuidado de salud, sea en el sector privado o en el sector público. Por ejemplo, un problema de interoperabilidad entre sanidad pública y privada. En segundo lugar, conviene analizar el grado de descentralización y elementos intermediadores existentes. Recordemos que si no hay descentralización, no se trataría de una tecnología blockchain o DLT, puesto que es su esencia. En tercer lugar, necesitamos analizar el grado de transparencia existente y cual se quiere alcanzar. En cuarto lugar, se requerirá analizar el consenso para la creación de nuevos bloques en la cadena y transacciones además de la validación ("o sello de validación" de los nodos participantes sean hospitales, centros médicos, personal sanitario, universidades, compañías farmacéuticas, farmacias, aseguradoras, gobiernos, administración públicas, etc.). Y en cuarto lugar, no olvidemos estudiar el sistema de identificación digital que se implantará, por ejemplo, un SII o sistema de identificación digital soberana. ¿Cómo identificar las blockchain entre ellas? ¿es posible? También caben preguntarnos: ¿cómo se identificarían las máquinas de IoTH? ¿entendemos aplicable eIDAS para blockchain? ¿y el RGPD) (ver cap. 5.2).

[330] Se decide optar por plataformas con soluciones en la nube como esta debido a la posibilidad que ofrece de desarrollar API para los participantes por medio de interfaz. Además los smart contract se pueden adaptar puesto que permanecen fuera de la cadena. No sólo eso, además funciona con lenguaje java por lo que no será necesario el manejo de Solidity (algo que considero importante). Técnicamente posibilita algo importante para la previsión de muchos participantes o nodos: la red pública puede procesar hasta 4.000 transacciones por segundo (ej. algo que se aprovecha entidades como VISA). Aunque tienen su propia moneda, vamos a partir de la idea de que la propia fundación europea contratista crea su propia moneda (tal y como hizo Hit Foundation). Para ver más info: https://nem.io/technology/

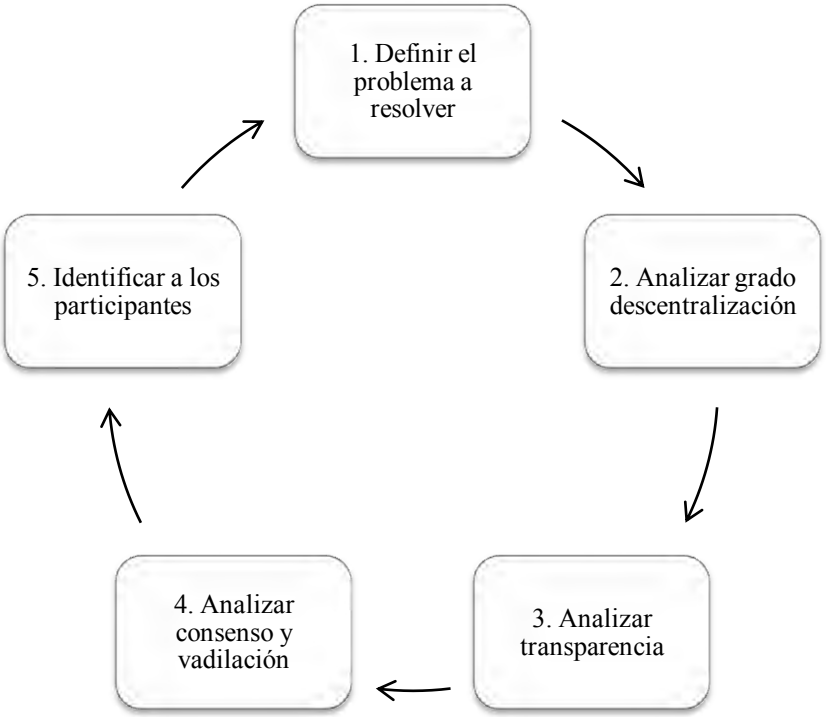


Tabla 17. Ciclo fases iniciales en la implantación de blockchain en salud.

Todas ellas son cuestiones que habrá que analizar antes de cualquier implantación, pero sobre todo, son pasos necesarios para implantar con éxito una blockchain.

ii. Determinar claramente quiénes son los participantes, qué activos habrá y qué transacciones se podrán realizar.

a. *Participantes:* pacientes y usuarios de eHealth, hospitales, centros médicos, personal sanitario, universidades, compañías farmacéuticas, farmacias, aseguradoras, gobiernos, administración públicas, etc. Son todos aquellos colectivos que van a jugar un papel en la cadena de bloques. Se contempla la posibilidad de implementar servicios de proveedores de identidad cuando sea apropiado. En este punto cabe preguntarse: ¿existirán grupos? ¿cuáles son los permisos que tiene sobre la red? ¿los usuarios o pacientes de *eHealth* podrán ver solo las transacciones en las que participe o tendrán acceso a más información? ¿podrá algún nodo o participante verificar en calidad de socio de confianza (ej. un seguro de salud)?

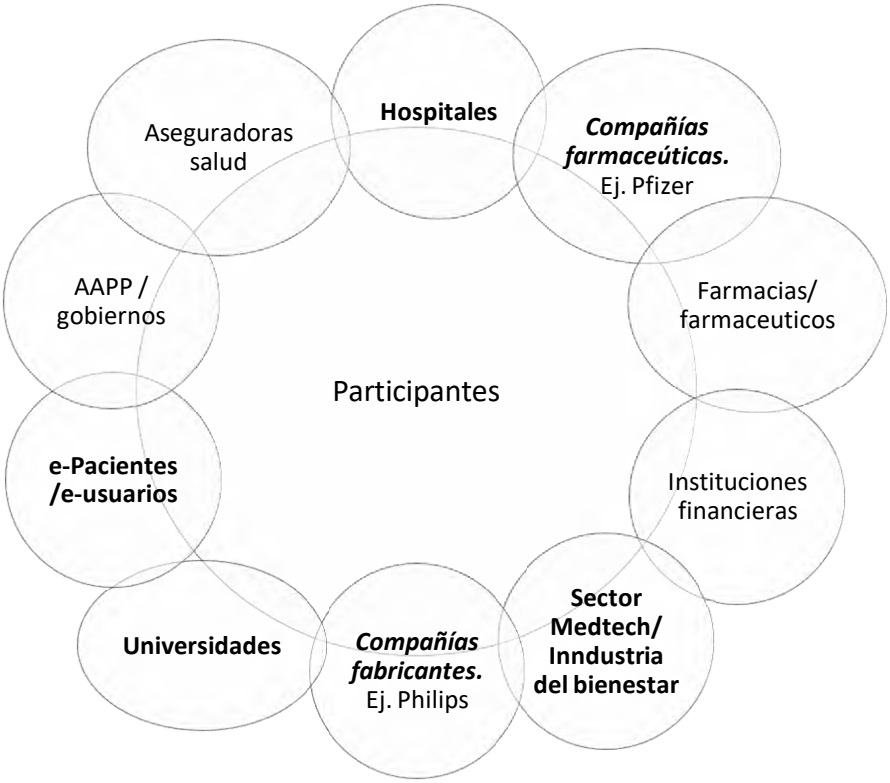


Imagen 36. Ejemplo de ecosistema de stakeholders con tecnología blockchain (ii).

b. *Activos.* ¿Qué se va a intercambiar? El individuo puede permitir el acceso, bien permitiendo la entrada al registro o almacenamiento de esos datos o siendo él mismo quien en un cuestionario los facilita en el propio monedero o wallet. A cambio recibirá los tokens que se hayan acordado en el Smart contract. Con dichos tokens, el individuo puede canjear servicios o bienes (descuentos, promociones seguros) o canjearlos por criptomonedas según el cambio oficial. Se espera que los individuos ganen más *tokens* con *datos validados* por personal de salud, por ejemplo, el registro de un diabético sería más valioso verificado por un profesional. Los titulares de datos existentes pueden enriquecer sus datos o ganar tokens al hacer que los datos sean accesibles.

c. *Transacciones o Intercambio de "token - información".* Por el momento sabemos quiénes son los jugadores y lo que se juega, pero faltarían las normas del juego. Gracias a ellas los participantes intercambiarán los activos (en nuestro caso, la información personal de salud). ¿Cómo se realizará el intercambio? Sobre la base de los *Smart contracts* donde el individuo podrá recibir fichas o *tokens* con el "valor" de los datos en las condiciones acordadas. Por ejemplo, *HIT Foundation* hace algo parecido:

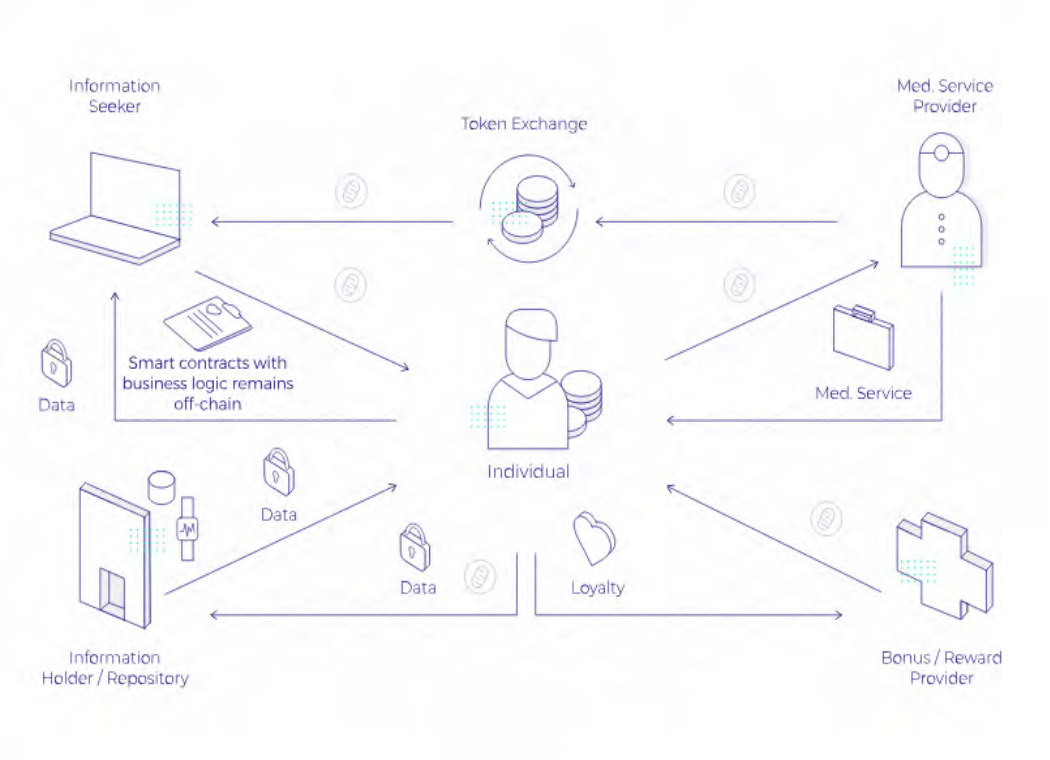


Imagen 37. Esquema transacciones en blockchain en Hit Foundation. Fuente: HIT Foundation

El individuo o titular de los datos, al registrarse (con su *wallet),* se le solicita que proporcione información básica sobre su estado de salud, por ej. peso y estatura. Y a partir de ese momento ya recibe *tokens*. Esta información se almacena fuera de la cadena de bloques y tiene derecho de acceso a través de su móvil o en el repositorio de datos médicos u otros sistemas de archivos distribuidos. Por su parte, los centros médicos pueden escribe sus consultas donde el individuo puede aplicar si le interesa a través del buscador de información (*information seeker*). Los tokens se pueden usar para canjear servicios o usar programas de fidelización. Con este sistema, no sólo pueden ganar *tokens* el paciente sino también los médicos o farmacéuticos, por ejemplo.

Balaji Srinivasan declaró (de manera irónica): *"cualquier cosa escasa será en última instancia tokenizada porque los beneficios de la digitalización y es aumento de la liquidez son muy grandes. Eso significa efectivo, acciones, bonos, materias primas, casas, autos, "bienes digitales de todo tipo, y tal vez tiempo humano en forma de token personal"*.

iii. Determinar casos de usos o utilidades posibles y sus transacciones[331].

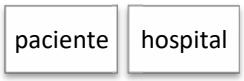
[331] Se toman en consideración algunos como los que contemplan el sistema de HIT Foundation. Vid. https://hit.foundation/wp-content/uploads/Whitepaper-HIT-Foundation.pdf (pp. 8)

a. *Investigación (ensayos clínicos e investigación pura).* Los investigadores tienen acceso directo a los posibles participantes del estudio mediante la búsqueda de sus metadatos que coinciden con los criterios de inclusión.

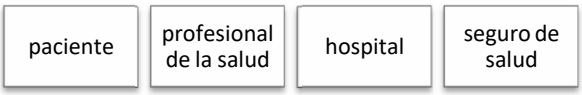
b. *Encuestas* contactando a los individuos directamente o por invitación (Código QR) y autenticándose.

c. *Modelos de pago por desempeño.* Los seguros y las industrias obtienen datos de resultados informados por los pacientes para controlar la efectividad de los tratamientos y, por tanto, el reembolso del tratamiento.

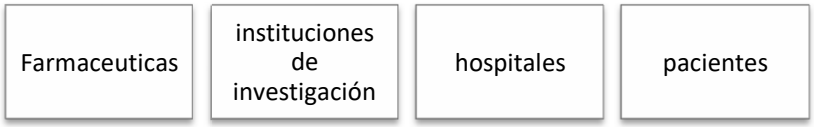
d. *Registro en el hospital.* Se escanea el código QR de un hospital cuando los pacientes ingresan en un hospital y se comienza a enviar datos de seguro y salud de los pacientes a los centros de información de los hospitales. El paciente recibe un token a cambio.



e. *Servicios de segunda opinión.* Los *médicos* (también) pueden ganar tokens dando comentarios, respondiendo al correo, revisando el tratamiento decisiones. Es información que interesaría al seguro de salud, por ejemplo.

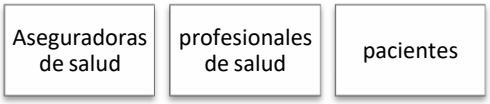


f. *ADN / biobanco.* Las muestras se pueden rastrear y obtener el consentimiento de los donantes. Los beneficios de este biobanco son la administrar la propiedad, privacidad y seguridad de datos personales muestras.



g. *Soporte de cumplimiento.* Los individuos reciben *tokens* cuando se definen *objetivos de salud* predefinidos que se incorporan en un *Smart contract*. Es una realidad. Hace poco la

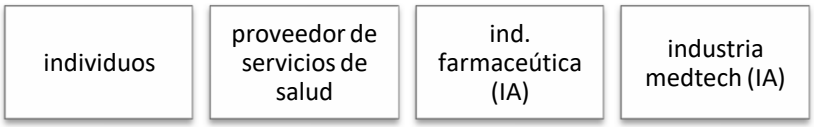
aseguradora del Corte Inglés anunció que bonificaría a los asegurados que caminaran[332]. La verificación puede provenir de un tercero, por ejemplo, un profesional de salud o por dispositivos inteligentes y conectados.



h. *Sistema de reembolso alternativo.* Se trataría de *cambiar "datos" por servicios de salud* facilitando el seguimiento de datos personales en diferentes lugares.

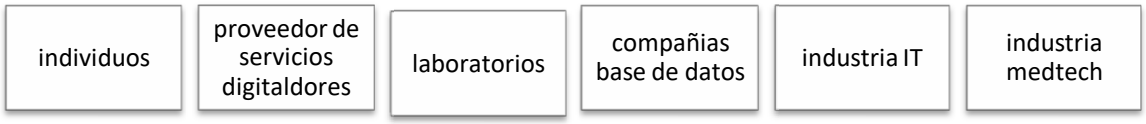
i. *Internet de las cosas (IoT) / dispositivos conectados.* Seguimiento de los datos de salud que se generan sin el conocimiento de los individuos y consentimiento por dispositivos conectados. Esto permitirá gestionar el acceso y el uso de los datos personales, su estandarización y una solución a los problemas de interoperabilidad.

j. Servicios de inteligencia artificial. Es una cuestión muy interesante. El token se podría usar como un pago para servicios bot, por ejemplo, interacción de control medicación, verificador de síntomas, explicación e interpretación de resultados de laboratorio.



k. Servicios de terceros. Los proveedores de servicios de salud pueden ser incentivados para aprovechar el sistema, por ejemplo, laboratorios que ofrecen autopruebas, proveedores que digitalizan registros en papel y documentos, comerciantes de bases de datos de pacientes (propietarios de grandes volúmenes de datos), industria de TI, pharma / medtech industria etc.

[332] Vid http://www.expansion.com/empresas/banca/2018/04/10/5accd666ca4741fa528b4635.html



l. *Seguimiento de la adopción de acuerdos de innovación.* Las partes interesadas pueden hacer un seguimiento de la adopción de innovaciones

En definitiva, la realización del estudio en sus 5 fases, el análisis de los elementos primordiales en todo sistema de blockchain (participantes, activos y transacciones) y la definición o el perfilado de los usos o utilidades que se podrán realizar en el marco de ese sistema son cuestiones necesarias a realizar a priori en el momento de decidir implementar un proyecto de blockchain. El análisis de fases también nos ayudará a determinar qué tipo de blockchain necesitaremos y la red o plataforma con la que desarrollaremos el proyecto.

5.7. Contexto futuro.

Antes de finalizar quisiera poner el foco de atención sobre dos tecnologías prometedoras que están en periodos de prueba y que impactarán, y por qué no, también el ámbito del cuidado de la salud.

i. De blockchain a IOTA

Lo que hace diferente a IOTA frente al resto de criptomonedas es que es la primera fuera del sistema Blockchain. En su lugar, usa Tangle, una plataforma de nodos interconectados en la que basa su funcionamiento. Cualquiera que quiera usar IOTA debe confirmar dos transacciones ajenas antes de poder enviar la suya[333]. En IOTA *no existe minería como en otras criptomonedas*, Esto significa que la resolución de problemas matemáticos que verifican transacciones, como en Bitcoin, no se puede hacer libremente, sino que solo la hacen los usuarios que quieren operar con IOTA. Esta verificación *se puede hacer con cualquier smartphone u ordenador*. No es necesario

[333] Vid. https://www.xataka.com/internet-of-things/iota-la-criptomoneda-sin-blockchain-que-ha-crecido-un-1000-en-un-mes

usar enormes granjas de minado o tarjetas gráficas de alta gama para ello, ya que al no haber minado no se va incrementando la dificultad como ha ocurrido con Bitcoin. Esto tiene una ventaja añadida: desaparece el enorme gasto energético que supone Bitcoin, por ejemplo.

Esta mecánica tiene otra consecuencia para el sistema: es resistente a la computación cuántica. Su estructura también hace que su escalabilidad sea "prácticamente infinita".

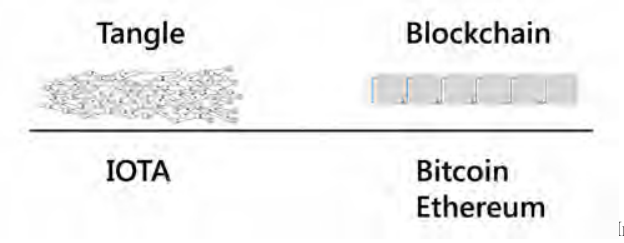


Imagen 38. Estructura IoTA. Fuente: Xataca

¿Y su aplicación en el cuidado de la salud?

En primer lugar, gracias a esta tecnología se podrá monitorizar al paciente de forma remota (a través de los propios dispositivos, smartphone u ordenadores). Sin embargo, asegurar y actuar estas corrientes de datos sigue siendo problemático. El protocolo de mensajería autenticada enmascarada de IOTA puede ayudar a asegurar estos flujos de datos utilizando los estándares modernos de interoperabilidad de la atención médica. En segundo lugar, IOTA puede aprovecharse *para transferir datos de pacientes cifrados granulares* entre hospitales sobre un paciente o su historia clínica completa sin tener que desarrollar una blockchain (y el coste que ello implica). En tercer lugar, facilita la integridad de los datos de investigación (lo que hace *blockchain*).IOTA, su criptmoneda es la primera que surge al margen de *blockchain* (no se obtiene minando como ocurre con *bitcoin* como resultado de la recompensa).

Veremos qué resultados aplicación se da en el sector que nos ocupa. Es claro que para decir qué usar conviene volver a analizar el problema u objetivo que tenemos sobre la mesa (ver capítulo 3.4) para determinar la mejor solución.

a. De blockchain a computación cuántica

Uno de los mayores temores que se encuentran en foros de expertos y simposios sobre blockchain tiene que ver con la incertidumbre que se puede crear la llegada de la computación cuántica y el miedo a que no existan medidas técnicas suficientes para asegurar la privacidad. Pero académicos de Nueva Zelanda afirman que es teóricamente

posible incorporar al *blockchain* la propiedad del entrelazamiento cuántico. *Esto significaría que la tecnología remontaría el tiempo y ofrecería una seguridad equivalente a la de la criptografía cuántica*[334].

[334] Ellos "sugieren que una cadena de bloques cuánticos podría resistir los intentos de piratería realizados mediante ordenadores cuánticos. El método que plantean estos científicos consiste en codificar la cadena de bloques en un estado temporal en el que los fotones entrelazados que componen estos bloques no coexisten simultáneamente. Este entrelazamiento cuántico en el tiempo, en oposición a un entrelazamiento en el espacio, proporciona una ventaja cuántica crucial, destacan estos investigadores". Vid. https://www.tendencias21.net/La-fisica-cuantica-revolucionara-la-tecnologia-blockchain_a44736.html

CAPÍTULO III. REGIMEN JURÍDICO DE LA PROTECCIÓN DE DATOS DE CLOUD COMPUTING E IoT DESDE EL ENFOQUE DE LA INDUSTRIA DEL CUIDADO DE LA SALUD DIGITAL

SUMARIO: 1. RÉGIMEN JURÍDICO APLICABLE AL USO DE CLOUD COMPUTING DE LA SALUD.- 1.1.Los sujetos jurídicos. 1.2. La contratación Cloud. 1.3.Transferencias internacionales y "BCR". 2. RÉGIMEN JURÍDICO APLICABLE AL USO DE IOT DE LA SALUD. 2.1. La importancia de la seguridad en la privacidad en IoT. 2.2. Los sujetos jurídicos implicados

"Nunca puedes cambiar las cosas luchando contra la realidad existente. Para cambiar algo hay que construir un nuevo modelo que haga que el modelo existente quede obsoleto".

(Buckminster Fuller)

Imaginemos un mundo en donde cada mañana después de levantarnos, acudimos al lavabo para lavarnos los dientes y por medio de nuestro cepillo de dientes inteligente a través de nuestra app en el smartphone, recibimos recomendaciones sobre medicamentos y suplementos nutricionales según nuestras necesidades y que además, pudiera analizar *muestras biológicas* (algo que nos puede alarmar, *a priori*) mensualmente y ceder (o "alquilar") esa información voluntariamente a los profesionales de salud especialistas en cuestión o incluso, enviar esa información a Internet (almacenada en un proveedor cloud) y comparar los datos de salud con investigaciones recientes médicas del área medico concreto.

Esto no es imaginación, es realidad. Ya en día, existe este tipo de empresas dedicadas a la atención sanitaria[335] que pretende aumentar la calidad de vida de pacientes o usuarios de *eHealth* gracias a IoT (e *blockchain,* como veremos en capítulos posteriores).

[335]Vid. https://www.coincrispy.com/2017/07/17/bowhead-dispositivo-blockchain/

Un hospital, un centro de atención primaria, una clínica dental, un laboratorio, una aseguradora son ejemplos de clientes de servicios de *cloud computing* como el almacenamiento de datos. Pero en este caso**,** ¿las personas titulares de los datos almacenados en cloud podrán entender cómo se protege sus datos? Hay que tener en cuenta que la mayoría de los contratos cloud son con contratos tipo y de adhesión, donde en pocas ocasiones cabe negociación alguna salvo que se traten de clientes grandes. El proveedor *cloud* subcontrata conforme van surgiendo las ofertas y lo hace en un contexto de continuo cambio.

Tras haber señalado escenarios a modo de ejemplo, es el momento de que analicemos el régimen jurídico aplicable al uso de cloud y de IoT de la salud, abordando cuestiones relacionadas con los sujetos jurídicos, la contratación y la seguridad de la información con el uso de estas dos tecnologías.

1. RÉGIMEN JURÍDICO APLICABLE AL USO DE CLOUD COMPUTING DE LA SALUD

1.1. Los sujetos jurídicos

Dentro del contexto de *cloud* debemos diferenciar varios *actores* con sus funciones correspondientes. El GT29 establecía algo muy importante respecto del RGPD, y es que la empresa proveedora cloud (encargado del tratamiento) que no se atenga a las instrucciones del responsable del tratamiento, será considerado responsable del tratamiento y estará sujeto a las normas específicas en materia de control conjunto. Ello se realiza precisamente para equilibrar la situación habitual de preeminencia del proveedor de la nube respecto del cliente (responsable del tratamiento).

Conceptos previos.

"Tratamiento de datos" es *"*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción"(Art. 4.2. RGPD).

"Dato personal" es *"*toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha personal" (Art. 4.1. RGPD).

"Datos relativos a la salud" son "datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud" (Art. 4.15 RGPD).

"Datos genéticos" son "datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona" (Art. 4.13 RGPD).

i. Cliente cloud ("responsable de tratamiento")

Un hospital , un centro de salud de atención primaria, una clínica dental, un laboratorio, una aseguradora de salud son ejemplos clientes potenciales de servicios de la nube. En los servicios cloud computing, los clientes también deberán tomar un papel activo[336]. A pesar del hecho de que la legislación de la UE sitúa claramente la responsabilidad de los datos perdidos o en peligro en las manos del que ostenta su propiedad, dos tercios (64%) considera que cualquier amenaza para sus datos dañaría

[336] Ya lo señalaba la Sentencia del Tribunal Supremo de 15 de julio de 2010, F.D. Décimo[336]: "Si el responsable del tratamiento, de conformidad con el artículo 17.2 de la Directiva, *debe elegir un encargado del tratamiento que ofrezca garantías suficientes* en relación con las medidas de seguridad técnica y de organización de los tratamientos que deben efectuarse, y *asegurarse que se cumplen dichas medidas***,** y si de conformidad con el apartado 3 del indicado artículo el encargado del tratamiento solo actúa siguiendo instrucciones del responsable del tratamiento, negar capacidad de disposición a éste en supuestos de subcontratación es una conclusión reñida con los más elementales criterios de la lógica.

más la reputación del proveedor de servicios en la nube que la de su propia compañía[337]. Para poder entender la visión práctica conviene repasar la *tipología de clientes de la nube,* que *Cloud Security Alliance* divide por un lado, s*egún el tamaño de la organización: (i) Multinacionale*s donde existen muchos datos repartidos en muchos países y cuentan con una herramienta que se adapta a las particularidades de cloud, basándose en el SLA (Acuerdo de Nivel de Servicio) que regulará la difícil relación jurídica y (ii) *Pymes*, las cuales confiarán en *la debida diligencia* del proveedor cloud. Por otro lado, s*egún el modelo de Cloud; (a)* Iaas donde el cliente se responsabiliza del acceso a apps, gestión de identidad de usuarios, como por ejemplo, *Amazon Web Servicies; (b) P*aaS donde el cliente gestiona las apps y por tanto es responsable del control de éstas. Por ejemplo, *Java; (c) S*aaS donde *el cliente delegará la responsabilidad en el proveedor* y en todo caso vigilará el SLA y dependerá de la información otorgada por el proveedor. Por ejemplo *Gmail.* Además, la situación jurídica del cliente de *nube privada* es diferente al de la *nube pública*[338].

En definitiva, estas cuestiones son relevantes porque el cliente es el responsable siempre independientemente del tipo de contrato que tenga, aunque no es lo mismo ser cliente de un servicio público de nube que de una nube privada, o no es lo mismo ser cliente de SaaS que de IaaS. Respecto a las obligaciones y derechos, el cliente elige qué datos van a ser objeto de tratamiento, a quién pertenecen dichos datos, qué finalidad tiene un tratamiento los datos previstos, si va a existir cesión o comunicación de datos a terceros etc[339]. Debe solicitar y obtener información sobre si intervienen o no terceras empresas (proveedores subcontratistas) en la prestación de servicios de *cloud computing*. De ser así, tiene que dar su conformidad a su participación, al menos delimitando genéricamente los servicios en los que participarán (por ejemplo, en el alojamiento de datos) e incorporar las *clausulas necesarias* para garantizar el derecho fundamental de protección de datos de las personas a lo largo del ciclo de vida de los datos.

---

[337] Vid. www.consultoras.org/frontend/aec/descargar.php?idf=21191

[338]CNIL. Recommendations for companies planning to use Cloud computing services. Recuperado de https://www.cnil.fr/sites/default/files/typo/document/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf

[339] En el antiguo Reglamento de desarrollo de la LOPD (Art. 20.2) ya señalaba la exigencia del responsable en *vigilar el cumplimiento por parte del encargado de tratamiento o proveedor cloud*, y a tener una *diligencia* a través de algún sistema que permitiera la realización de controles periódicos. Como propietario de la información debía analizar los riesgos sobre el ciclo de vida de la misma y los activos.

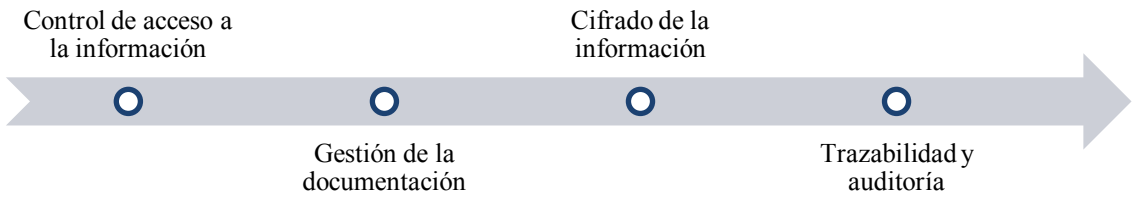


Imagen 39. Ejemplo de ciclo de vida del tratamiento en almacenamiento de datos. Fuente propia.

Dicho con otras palabras, el cliente tiene una doble obligación; primero, elegir un proveedor, y segundo, asegurarse de que cumple la normativa. Por otro lado, no será poco frecuente que se den situaciones donde hayan varios responsables. En el Dictamen 1/2010 del GT29[340], el ejemplo 15 puede resultar de nuestro interés y aplicación para esta cuestión. Éste está orientado a plataformas de gestión de datos de salud de un Estado miembro donde una autoridad pública establece un punto de conmutación nacional que regula la intercambio de datos de pacientes entre los proveedores de asistencia sanitaria (clientes cloud). Según la GT29, "la pluralidad de los responsables de asistencia sanitaria (decenas de miles) resulta en una situación tan poco clara para las personas a las que se refieren los datos (pacientes) que la protección de sus derechos estaría en peligro". Nos preguntaríamos ¿dónde se dirigirían los titulares/pacientes para ejercitar sus derechos? El grupo de trabajo parecía no tenerlo claro a priori, no obstante, señaló que "la autoridad pública (cliente cloud) es responsable del diseño real del tratamiento y de la forma en que se utiliza". En este contexto, puede afirmarse que la responsabilidad solidaria de todas las partes debe ser considerado como un medio para eliminar las incertidumbres, y por lo tanto sólo en la medida en que sea una asignación alternativa, clara e igualmente efectiva de obligaciones y responsabilidades no han sido establecidas por las partes involucradas o no se derivan claramente de circunstancias fácticas.

ii. Proveedor cloud ("encargado de tratamiento").

Dropbox, Amazon Web Services, Microsoft, IBM, SAP, Salesforce son ejemplos de proveedores de servicios de la nube. El GT29 establece que el concepto de encargado de tratamiento por el que se determina en función de dos condiciones básicas: ser una entidad independiente del responsable del tratamiento y realizar el

[340] GT29. Opinion 1/2010 on the concepts of "controller" and "processor". WP 169. Aprobado el 16 de febrero de 2010). Recuperado de https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf#page=26&zoom=100,0,694

tratamiento de datos personales por cuenta de éste[341]. Señala algo determintante: "actuar en nombre de otra persona" significa servir a los intereses de otra persona y recuerda el concepto jurídico de "delegación". "En el caso de la ley de protección de datos, un encargado es llamado a aplicar las instrucciones dadas por el responsable del tratamiento, al menos en lo que se refiere a la finalidad de el tratamiento y los elementos esenciales de los medios. Un encargado que va más allá de su y adquiere un papel relevante en la determinación de los fines o los medios esenciales. de procesamiento es un responsable (conjunto) en lugar de un encargado". No obstante, "la delegación puede implicar un cierto grado de discrecionalidad en cuanto a la mejor manera de servir a los intereses del responsable, permitiendo al encargado elegir el más adecuado medios técnicos y organizativos".

En el Dictamen 1/2010, en el ejemplo 16, se señala el caso de proveedores de alojamiento cloud como encargados de tratamiento donde señala que en caso de que éste "siga procesando los datos *para sus propios fines* contenidos en las páginas web será responsable del tratamiento en lo que se refiere a dicha tratamiento de información específico. Este análisis es diferente al de un ISP que proporciona acceso al correo electrónico o a Internet. Por tanto, ¿dónde está el limite de las dos figuras en cloud? Los proveedores cloud eligen los medios, por regla general, es decir el objeto o la duración son, en cambio es el cliente el que elige qué datos se ponen en *cloud.* El GT29 lo reafirma al establecer que un encargado que va más allá de su mandato y adquiere un papel relevante en la determinación de la fines o los medios esenciales de procesamiento es un responsable ("*joint controller"*) en lugar de un encargado. En todo caso, será el cliente cloud (por ejemplo, un laboratorio) quien se encargará de implantar las medidas de anonimización para los datos de salud de categoría especial.

Respecto a los derechos y obligaciones, mencionar tal y como quedó reflejado en la Sentencia de la AN 20 Septiembre de 2002: "el encargo de tratamiento se ampara en la prestación de un servicio que el responsable del tratamiento recibe de una empresa ajena a su propia organización y que le ayuda en el cumplimiento de la finalidad del tratamiento de datos consentida por el afectado"[342].La jurisprudencia[343] dio un paso

[341] *Ibídem*.

[342] Sentencia de la AN, Sala de lo Contencioso-administrativo, Sección 1ª, 20 sep. 2002 (Rec. 150/2000).
343 Vid. Sentencia de la Audiencia Nacional, Sala de los Contencioso-administrativo, sección 1ª, 16 mar. 2006 (Rec. 427/2004).

adelante y va más allá. En la obligación del *contrato formal* está la necesidad de detallar las *condiciones* que se establecen en dicho precepto y que garantice la seguridad de los datos impidiendo el acceso de los mismos a terceros y otras como la *identificación geográfica* de los agentes operadores, ley aplicable y jurisdicción; así como una remisión de las *medidas de seguridad* aplicables, el *compromiso de responsabilidad* de cualquier incumplimiento normativo y la finalidad de los *subencargos*. En función del tipo de servicio, el *grado de responsabilidad* del proveedor cambiará[344]. Como se puede observar algunas de las condiciones contractuales se han modificado y se ven desfasadas con la normativa del RGPD en mano.

iii. Subcontratistas ("subencargados").

El art. 28.4 RGPD establece que:

> "Cuando *un encargado del tratamiento recurra a otro* encargado *para llevar a cabo determinadas actividades de tratamiento por* cuenta del responsable, se impondrán a este otro encargado, *mediante contrato u otro acto jurídico* establecido con arreglo al Derecho de la Unión o de los Estados miembros, las *mismas obligaciones* de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento.
>
> Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial *seguirá siendo plenamente responsable* ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado".

Por tanto, se impondrán a los subencargados las mismas obligaciones de protección de datos que se estipularon en el contrato entre responsable y encargado (medidas técnicas y organizativas). Y en todo caso, cuando el subencargado incumpla contractualmente, el encargado responderá frente al responsable. Por ello, es necesario que el encargado de tratamiento se asegura de que toma las medidas adecuadas para que el subencargado cumpla contractualmente acorde con la nueva normativa.

[344] Pero, ¿como deberá ser el tratamiento? Puede quedar delimitado y concretado por la actuación del encargado por el propio responsable del fichero (ej. contrato de adhesión tipo) o puede dejar un cierto margen de maniobra respecto a cómo realizar su función en base a los intereses de dicho cliente cloud. Por tanto, hace más de una década las condiciones contractuales obligatorias para la jurisprudencia quedaron definidas en; (i) delimitar la finalidad de la comunicación; (ii) prohibición expresa al proveedor de no comunicar a terceros; (iii) implementar las medidas de seguridad; (iv) delimitar el tiempo contractual; (v) especificar lo que se hace al final del ciclo de los datos; (vi) contar con clausulas de confidenciales dirigidas a proveedores; (vii) obligación de comunicar al cliente cuando los usuarios quieren ejecutar los derechos ARCO; (viii) establecer documento de seguridad.

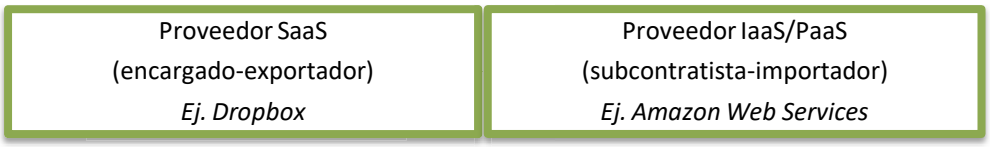


Imagen 40. Ejemplos de Subcontratación proveedor Saas y Iaas/Paas. Fuente propia.

Por otro lado, el art. 29 RGPD establece que:

> "El encargado del tratamiento y cualquier persona que *actúe bajo la autoridad del responsable o del encargado* y tenga ***acceso a datos personales*** *solo podrán tratar dichos datos siguiendo instrucciones del responsable*, a no ser que estén obligados a ello en virtud del Derecho de la Unión o de los Estados miembros".

Esto implica que los subencargados que tengan acceso a datos personales, únicamente podrán realizar tratamientos siguiendo las instrucciones del responsable salvo que existan otras obligaciones de derecho nacional o comunitario que les afecte.

iv. Titulares de los datos personales.

Los titulares de datos personales en cloud somos cualquiera de nosotros que estamos dentro de la base de datos de una clínica dental, de un hospital (público o privado) o en la base de datos de una tecnológica de e-Health por medio de una aplicación móvil.

Según el *Cloud Compliance Report* de CSA[345], las personas afectadas por el tratamiento de sus datos se enfrentan a dos casos. En el primero, sus datos pueden ser tratados por una empresa española que subcontrata parte de sus servicios en cloud y en este caso, es poco probable que conozca la existencia de la transferencia internacional y, frente a él, toda la responsabilidad es del responsable. Y en el segundo, la persona que puede contratar directamente unos servicios cloud como es el correo electrónico, almacenamiento de datos, o capacidad computacional (IaaS). En este caso, la persona física debería tener unas precauciones similares a una empresa usuaria con la diferencia que su capacidad negociadora va a ser muy reducida y en algunos casos las condiciones pueden resultar abusivas. En todo caso, se podrían concebir al titular de datos desde una visión como "consumidor" (y parte directa en los contratos).

[345]Vid. https://cloudsecurityalliance.org/

v. Nuevas figuras.

AWS Services Broker, Appirio, Cloudmore, Bluewold son ejemplos de una nueva figura; el broker cloud. Éste toma un papel esencial dentro de la negociación contractual como intermediario y, en otros casos, éste puede denominarse "agregador" cloud y ofrecer al cliente una API y una interfaz de usuario facilitando el uso. Pero en otros, el bróker puede habilitar cifrado, la portabilidad, la eliminación de datos duplicados y asistir en la gestión del ciclo de vida de los mismos, por tanto estaría accediendo a los datos. También podemos considerar como otra figura a los "auditores"[346].

1.2. **La contratación Cloud.**

Para hablar de *contratación cloud* tenemos que nombrar el resto de fuentes de las obligaciones del cliente cloud que estarán contenidas en fuentes externas (derecho positivo y normal del cliente cloud en virtud de su localización); normas y políticas corporativas (ej. ISO 27001); y obligaciones contractuales. Centrándonos en la fuente última abordaremos algunas cuestiones generales a continuación. Por un lado, existe un *componente cultural-educacional.* Los proveedores necesitan de "educación contractual" y los legisladores requieren de "educación sobre la tecnología cloud y estructuras del negocio". Por otro lado, el *factor geográfico es determinante*. Como establece el profesor *Schwartz* la diferencia entre la legislación en materia de contratación cloud entre la UE y EEUU, es clara[347]. En el primer caso, la contratación se basa -mayoritariamente- en la *"Law of Terms of Service", (*es decir, *"take it or leave it)"*. Pero aunque EEUU tenga esa limitación, Estados como el de California contará con una nueva ley de privacidad que entrará en vigor en 2020[348] con características similares a nuestro RGPD. Además, el FCT (Comisión Federal de Comercio norteamericano) no ha dejado de pronunciarse en cuestiones respecto a los proveedores y clientes cloud y sus obligaciones. Es de destacar por cuanto nos interesa el *caso*

[346] El art. 51.1 y 51.2 LOPDGDD señalan que "La AEPD desarrollará su actividad de investigación a través de las actuaciones previstas en el Título VIII y de los planes de auditoría preventivas. La actividad de investigación se llevará a cabo por los *funcionarios* de la AEPD o por *funcionarios ajenos a ella habilitados* expresamente por su Presidencia".
[347] Schwartz, Paul M. (2013) Information privacy in the cloud . *University of Pennsylvania Law Review*. Vol. 161. Págs. 1653-1661.
[348] Vid. https://www.caprivacy.org/

GMR[349] por su implicación con datos sanitarios y el papel de los actores. Y en el segundo caso, la legislación europea, no permite contraerse y cuenta con *"estándares inmutables"*. Según el profesor *Schwartz*, la lógica de la legislación europea estará en proteger a los "terceros" (titulares de datos personales) de la falta de transparencia y de la asimetría de la información respecto a lo que se trata de ellos. Además, propone para acabar con el entramado regulatorio actual con las siguientes iniciativas: (i) desarrollar un modelo de clausulas contractuales para la seguridad, transparencia y calidad de datos con una creación de principios claros y armonizados sobre la "rendición de cuentas de los proveedores*"*[350] y (ii) desarrollar un conjunto de *estándares* con los *contract terms* con el objeto de poner en práctica los principios que impulsa la Comisión Europea.

Y por último es de destacar la importancia del papel de la *autonomiá y voluntad de las partes.* En este sentido, el CSA (*Cloud Securtity Alliance*), establece que Cloud es un "modelo de servicios TIC en el contexto de una relación B2B, la cual es en principio "libre" en virtud de la *autonomía de la voluntad* que rige la contratación". Un acuerdo entre el proveedor y el cliente del servicio cloud no debería ser estático (al igual que su naturaleza técnica) sino que debería estar sujeto a las necesidades del consumidor. Instituciones sanitarias, organizaciones aseguradoras y administraciones públicas (potenciales y potentes clientes *cloud*) están esforzándose para colaborar y producir su "propio" estándar de términos y condiciones. Situación diferente afrontan las pymes el poder de negociación es más escaso. Pero, ¿por qué no podrían los legisladores fomentar una mayor gama de servicios disponibles en la nube con

---

[349] En primer lugar, la *posición del titular de datos ("consumidor") en el contexto contractual en EEUU.* Para *Solove*, cuando una entidad –como un hospital- comparte datos con proveedor cloud, no siempre estos datos estarán protegidos. El consumidor no es parte directa de estos contratos y en ocasiones no puede tener ni acceso. Pero la protección jurídica la encuentra en el art. 5 de la Ley de la FTC que prohíbe las prácticas comerciales desleales y engañosas, como por ejemplo, no permitir elegir de manera adecuada (con contrato) y supervisar el proveedor cloud[349]. En segundo lugar, se encuentra la *postura del encargado ded tratamiento ("cliente cloud") en el contexto contractual.* GMR Transcription Services Inc., contenía información personal (formato audio) como historias clínicas o notas psiquiátricas y no verificó adecuadamente su proveedor cloud (Fedtrans) ni implementó medidas de seguridad razonables y apropiadas, ni actuó con la "diligencia debida" antes de contratarlo. Para la FTC, las empresas cliente cloud tendrán deberes de gestión, elección, contratación y supervisión de los proveedores cloud. Y en tercer lugar, está *la posición de los proveedores cloud como "administradores de datos"*. Solove señala que "los recopiladores de datos deben actuar como *administradores de consumidores* cuando la organización comparte información con un proveedor de la nube". Él señala que desafortunadamente no todos los acuerdos de servicios de cloud (CSA) son adecuados por diversos motivos; falta de claridad, dificultad de negociación diferente a un contrato ordinario, falta de conocimiento en privacidad y seguridad.

[350]Ver en línea: http://ec.europa.eu/information_society/activities/cloudcomputing/docs/quantitative_estimates.pdf.

diferentes conjuntos de términos[351] que los individuos pudieran evaluar y elegir el mejor servicio satisfaciendo sus necesidades y protegiendo sus derechos?[352]

Analizadas estas cuestiones, pasemos a preguntarnos; ¿qué es el contrato en *cloud computing en España*? Es la expresión de la relación jurídica entre el cliente y el proveedor y requiere de la exigencia de "*mayores garantías" (*STS 15 de junio de 2010, FJ 10)[353].

1.2.1. Cuestiones particulares.

i. La negociación cliente VS proveedor cloud.

La negociación contractual[354] procedente del contrato o derivado de él, es un proceso que incluye dos o más partes, con intereses comunes, pero a su vez en conflicto que voluntariamente se reúnen para presentar y discutir propuestas comunes con el propósito de llegar a un acuerdo. Pero según una encuesta recogida por el CIF (*Cloud Industry Forum*, 2011)[355], encontró que mientras el 48% de las organizaciones encuestadas ya estaban usando cloud, solo el 52% de los clientes habían negociado sus contratos pero existía oportunidad de negociar los *"click-throug"* o contratos clickwrap. La mayoría de los contratos cloud son así sobre todo si se trata de cloud pública donde no cabe margen de negociación prácticamente. El discurso cambia si nos encontramos con servicios de cloud privada o híbrida, ya que los servicios se hacen a medida negociando el propio "*service legal agreement"* o acuerdo de nivel de servicio. La tendencia es pensar que cuanto más grande sea, el cliente mayor poder de negociación

[351] Con los servicios de nube privada que gestiona personalizados sobre infraestructura dedicada, los proveedores pueden ser más flexibles con las condiciones contractuales. Sin embargo, el consumo masivo de los servicios de nube pública en infraestructura compartida es una propuesta muy diferente. Son baratos, ya que están estandarizados. Los clientes quieren el precio más bajo, pero las más altas especificaciones y características (la vigilancia ubicación o derechos de auditoría), obligando a los proveedores a aceptar más responsabilidad e incurrir en el gasto de actualizar su infraestructura.

[352] Por ejemplo con: (i) *Nubes públicas* (más económicas) para cuando no hayan datos personales ni información confidencial; (ii) *Nubes privadas o comunitarias* (más caras) con alta seguridad y auditables dirigidas a sectores específicos como los sanitarios. Estos clientes posiblemente tengan más recursos informáticos de las estructuras de cloud que el pequeño consumidor o las PYME para evaluarles.

[353] En el recurso de legalidad frente a este precepto, que es desestimado y se da por buena la obligación de que el encargado del tratamiento comunique al responsable la necesidad de subcontratar y con quién pretende hacerlo.

[354] Según Berlew y Moore (1987) "la calidad de la negociación se mide por el impacto y la influencia que ejerzamos en la contraparte y no sólo por la intención que tengamos en la misma".

[355] Cloud Industry Forum, Cloud UK. (2011) Paper Three – *Contracting Cloud Services: A Guide to Best Practices.* Recuperado de http://www.cloudindustry forum.org/downloads/whitepapers/cif-white-paper-1-2011-cloud-uk-adoption-andtrends.pdf

contractual tendrá. Pero no siempre es así[356][357]. Pero quienes tienen más capacidad en la negociación son los *"integrator"* o facilitadores, como son por ejemplo, *IBM's Smart Enterprise Cloud* o *HP's Enterprise Cloud.* Piénsese en contratar paquete Office365 con con integradores de infraestructura cloud con sus SLA y términos.

ii. La subcontratación de proveedores en la cadena de suministro.

Según *Compuware*[358] un 20% de las empresas no protege los datos de los clientes antes de compartirlos con empresas subcontratadas. La AEDP ha reconocido en más de una ocasión que las características particulares de los contratos de *cloud computing* impiden aplicar literalmente los requisitos de la subcontratación. En el 2016, la Comisión Europea modificó[359] las decisiones relativas a las clausulas contractuales tipo para las transferencias europeas adaptándose a las contexto del RGPD y de los antecedentes como fue la Sentencia Schrem en 2015[360].

El proveedor *cloud*[361] subcontrata conforme van surgiendo las ofertas, por tanto, lo hace en un contexto de continuo cambio y eso le impide incluir en su anexo la lista de todos y cada uno de sus subproveedores en tiempo real. En este tipo de casos, lo que recomienda la AEPD, es publicarlo en la web, ya que eso le permitirá al proveedor *cloud* "actualizarlo" de una manera más dinámica y periódica. Pero, ¿qué papel tienen

[356] Por ejemplo, el prototipo de la web de servicios públicos del gobierno de Reino Unido (Alpha.gov.uk) fue creado por *Amazon* (IaaS) con términos y condiciones estándar y sin negociación alguna. Lo mismo pasó con un modelo piloto para el Consejo del condado de *Warwickshire* de *Google Apps* (SaaS) (2011) con unas condiciones estándar de Google.

[357] Hall, K. (19 de septiembre de 2011). Warwickshire County Council Signs Google to Pilot G-Cloud Email Service. *Computerweekly.* Recuperado de http://www.computerweekly.com/news/2240105636/Warwickshire-County-Council-signs-Google-topilot-G-Cloud-e-mail-service

[358] Vid. http://www.ciospain.es/seguridad/nueva-ley-de-proteccion-de-datos-de-la-ue-donde-estan-las-dificultades-para-cumplirla

[359] COMISIÓN EUROPEA, DECISIÓN DE EJECUCIÓN (UE) 2016/2297 DE LA COMISIÓN de 16 de diciembre de 2016 por la que se modifican las Decisiones 2001/497/CE y 2010/87/UE, relativas a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016D2297&from=ES

[360] Ver https://anf.es/pdf/MODELO-DEFINITIVO-AEPD_Contrato-encargado-subencargado-21-03-2012.pdf. (Ya en el 2012, la APED señala las *clausulas contractuales* necesarias de encargados para subencargados, en los que se debía rellenar los apéndices 1-datos del exportador, del importador indicando a las actividades de la transferencia, categoría de interesados, de datos y las operaciones de tratamiento- y en el apéndice 2 -las medidas de seguridad técnicas y organizativas como el cifrado, backup, etc).

[361] Pérez Campillo, L. (12 de diciembre de 2016). Cloud Computing: Gestión de riesgos y data protection; ¿cómo evitar pagar los platos rotos? *ItUser.* Recuperado de https://www.ituser.es/opinion/2016/12/cloud-computing-gestion-de-riesgos-y-data-proteccion-como-evitar-pagar-los-platos-rotos

los sujetos jurídicos en esta relación contractual de subcontratación de servicios de *cloud computing?; ¿hasta qué punto son subencargados los subcontratistas?¿se deberían también considerar subcontratistas aquellos que dan alojamiento a una máquina virtual llena de datos inteligibles(cifrados y fragmentados)*[362].

1.2.2. Las elementos y garantías contractuales generales en cloud.

i. Según GT29

El GT29 en el *Dictamen 05/2012*[363] estableció una serie de derechos y obligaciones contractuales en para ser incorporadas y así garantizar un efectivo cumplimiento:

Imagen 41. Derechos y obligaciones a ser incluidos en el contrato cloud.

ii. Los SLA ("Service Level Agreement")

[362]Por ejemplo, pensemos en la virtualización a través de VMware creando una máquina virtual donde se pueden añadir un sistema Linux o un sistema XP. Si consideramos a *VMware* como subcontratista de cloud; ¿ se podría considerar un tratamiento de datos al acceso inteligente del propietario del servidor a la máquina virtual? En base a la normativa aplicable se establece que el operador de telecomunicaciones que no preste servicios de acceso a la red directamente al abonado, podría considerarse prestador de servicios *sin acceso directo a datos personales* de los titulares o usuarios, al tener prohibido la conservación de ningún dato que revele el contenido de las comunicaciones (Art.3.3 Ley 25/2007). Pero en el caso de que éste preste servicios de *hosting de correo electrónico o disco duro virtual*, por ejemplo, debería considerarse encargado y por tanto cumplir, los requisitos del artículo 28.3 RGPD.

[363] No obstante, el Grupo de Trabajo en la nota de prensa de 1 de julio de 2012, referente al citado Dictamen señaló que *"(...) es posible que no puedan aplicar las medidas técnicas y organizativas necesarias para garantizar, por ejemplo, la disponibilidad y confidencialidad de los datos, de los que el cliente de los servicios en la nube continúa siendo jurídicamente responsable conforme a la legislación de la UE"*. Por lo que el grupo de trabajo mantenía una posición realista y pragmática respecto a la dificultad existente. Es por ello que las organizaciones que deseen utilizar servicios de computación en nube deberán realizar un análisis exhaustivo y riguroso de los riesgos.

Los SLA se tratan de contratos estáticos y predefinidos, incompletos y ambiguos para el cliente, protegen los intereses de los proveedores y sus bases en el SLM. En ellos se incluyen indicadores que serán necesarios para medir el servicio y la métrica (tiempo de disponibilidad, servicios afectados…etc.). El NIST lo define como lo que representa *"al nivel de servicio que se va a dar al cliente y que en caso de no cumplimiento debería de existir cierta compensación"*. El *C-SIG* (Selección del Grupo de la industria de la nube en la Comisión Europea) ha creado una subcomisión llamada *C-SIG SLA* que está trabajando y desarrollando pautas de normalización para los SLA[364] [365]. Estos contratos deberían contener algunas clausulas como:

1. *Cláusula de responsabilidad.* El proveedor ha de hacerse responsable frente al cliente de cualesquiera daños o perjuicios o de cualquier reclamación que pudiera surgir o que traiga causa en la suscripción del contrato.
2. *Cláusula de privacidad y protección de datos.*
3. *Cláusula de resolución anticipada.* Se recomienda negociar e intentar eliminar clausulas de penalización o "compromiso de permanencia" al igual que exista un compromiso por parte del proveedor a su colaboración en una posible migración a una supuesta nueva infraestructura.
4. *Cláusula de mecanismos de resolución de conflictos*. Se ven necesarios estos sistemas dada la deslocalización de servicios, la múltiple concurrencia de jurisdicciones, la poca capacidad de la administración de justicia, la escasa celeridad y especialidad para resolver conflicto dentro del ámbito tecnológico. El arbitraje se presenta como una opción viable, alternativa y necesaria.
5. *Cláusula ley aplicable y jurisdicción.* En la práctica, la parte contractual "más fuerte" es la que impone el fuero que más le beneficia. Lo normal es que la jurisdicción y la ley aplicable sea la misma.
6. *Cláusula de confidencialidad***.** Lo ideal es que "información confidencial" sea un concepto muy amplio y englobe todo lo posible como *información del cliente, de sus empresas, programas, su procedimiento de desarrollo, su know-how, su estructura interna, su tecnología, precios, ventas, información financiera, documentación, diseños, invenciones, tecnologías, precios, ventas…etc.* También se deberá prever una clausula donde se indemnice al cliente por los daños causados -al igual que cláusulas penales con tal concepto-.

[364] Comisión Europea (2014). Cloud Service Level Agreeement Standardisation Guidelines. Recuperado de https://ec.europa.eu/digital-single-market/en/news/cloud-service-level-agreement-standardisation-guidelines

[365] Es de mencionar el gran impulso que se ha realizado gracias a la "Estrategia Europea de *Cloud Computing*" promovido por la Comisión Europea y que se ha manifestado en programas como el de *SLA-AID,* un programa gratuito con directrices específicas basadas en un cuestionario dirigido para el sector privado con lenguaje claro. A mi parecer, además de determinar métricas, se debería completar con contenido de PLA y las obligaciones para encargados de tratamiento a partir del 25 de mayo de 2018 con el RGPD. Tampoco he podido encontrar mención expresa a particularidades jurídicas derivadas de la cadena de suministro en cloud computing. Ver en http://www.sla-ready.eu/news/sla-aid-now-available

7. *Cláusula de Propiedad intelectual.* Se deberá fijar que tanto el acceso al contenido generado por el cliente por parte del proveedor, como la reproducción, copia, modificación, comunicación pública, distribución y cualquier cesión suponen infracciones de la propiedad intelectual al cliente.
8. *Cláusula de Auditabilidad.* Se pueden incluir clausulas de auditoria de cumplimiento normativo, de cumplimientos de estándares y buenas prácticas, de políticas internas y código ético o de control control de cumplimiento contractual. Deberán contemplarse cuestiones como el alcance geográfico, la capacidad de auditar a subcontratistas, que sean realizadas por terceros independientes y si suponen gastos por parte de los proveedores o subproveedores. Además, será importante averiguar si va a tener implicación los resultados de la auditoría en el contrato.
9. *Cláusula de Seguridad.* Puede ser recomendable un análisis de riesgos previo como punto de partida a la contratación, así de esta manera se determinará cuales son y qué estrategia se podrá tomar. Cada empresa tiene un nivel de vulnerabilidad diferente.

iii. Los PLA ("Privacy Level Agreement").

Estos acuerdos, a diferencia de los anteriores, se usarán para dirigir las prácticas en relación con la *privacidad y la protección de datos de carácter personal*[366]. El proveedor de servicios *cloud* deberá concretar y definir el nivel de protección de datos que se compromete a mantener. Según el CSA[367], un proveedor puede contar con diferentes PLA dependiendo del tipo de servicio que vaya a prestar, las diferentes ofertas o prácticas o mercados. Además, establecen que un PLA puede apuntar o hacer referencia a otro documento sobre aspectos más específicos como el marco temporal, alcance, forma o propósito del tratamiento de datos personales, así como el tipo de datos tratados. Esta información deberá ser consensuada y recabada con el cliente. Además, optar por tomar un esquema de PLA a nivel mundial puede constituir un estándar muy valioso respecto a las herramientas de transparencia y responsabilidad allá donde puedan existir transferencias internacionales.

Según el *CSA (Cloud Security Alliance)* está formado por algunos aspectos como los siguientes:

1. La *identidad del proveedor* (y representante local en la U.E.), su función-como co-responsable, encargado o sub-encargado- y la información de contacto del DPO y del ISO.

---

[366] El PLA parece encajar perfectamente en la acción clave 2 de la Estrategia Europea sobre Cloud Computing: "la identificación y difusión de las *mejores prácticas* en materia de modelos de condiciones contractuales acelerará la aceptación de la computación en nube, al aumentar la confianza de los clientes potenciales. La adopción de medidas adecuadas sobre las cláusulas contractuales puede *resultar útil asimismo en el ámbito crucial de la protección de datos."* (…). Ver Comunicación de la Comisión al Parlamento Europeo, al Consejo, Al Comité Económico y Social Europeo y al Comité de las Regiones. COM (2012) 529 final. "Términos y condiciones de contratación seguras y justas de la Estrategia Europea de Cloud Computing".

[367] Ver en línea https://www.ismsforum.es/ficheros/descargas/acuerdo-de-nivel-de-privacidad1374159133.pdf

2. Las *categorías de los datos personales* que el cliente tiene prohibido transmitir o tratar en la nube. Ej. datos relacionados con la salud.
3. *Formas en las que los datos serán tratados.* Si el proveedor es encargado de tratamiento en cloud computing debe incluir información detallada sobre el alcance y las modalidades que el cliente puede dar instrucciones al proveedor: Especificar la ubicación de los data center, dónde y cómo se podrán almacenar, duplicar, respaldar y recuperar; identificar los subcontratistas y sub-encargados que participan, la cadena de responsabilidades, y el enfoque utilizado para garantizar que se cumplen los requerimientos de protección de datos.
4. Indicar *si los datos pueden ser transferidos*, copiados y /o recuperados de forma transfronteriza, en el curso normal de las operaciones o ante una emergencia.
5. Especificar las *medidas técnicas, físicas y organizativas* implementadas para proteger los datos personales contra la destrucción, accidental o ilícita, y la pérdida accidental; alteración, uso, modificación, difusión o acceso no autorizados; y contra toda forma ilícita de tratamiento.
6. Indicar si el cliente tiene la opción *de supervisar, monitorizar y/o auditar* las medidas apropiadas de seguridad descritas en el PLA..
7. Especificar si y cómo se informará al cliente de las *violaciones de datos* de carácter personal.
8. Especificar los formatos, la preservación de relaciones lógicas y cualquier coste asociado con la *portabilidad de datos*, aplicaciones y servicios. Describir las políticas de retención de datos del proveedor y las condiciones para devolver los datos de carácter personal y su destrucción una vez el servicio ha finalizado.
9. Describir qué *políticas y procedimientos de responsabilidad* ha desplegado el proveedor para garantizar y demostrar el cumplimiento legal, tanto por su parte, como por la de sus subcontratistas y socios de negocios, incluyendo la adopción de políticas internas y mecanismos que garanticen dicho cumplimiento legal.
10. Especificar *cómo cooperará* el proveedor con el cliente cloud para garantizar el *cumplimiento legal* de las disposiciones de protección de datos aplicables. Ej.: Para permitir que el cliente garantice el ejercicio de los derechos de sus usuarios (acceso, rectificación, cancelación, bloqueo y oposición).
11. Describir los procesos existentes para gestionar y responder a *las peticiones de revelación de datos de carácter personal* por parte de las autoridades competentes, con especial atención al procedimiento de *notificación a los clientes.*
12. Indicar las *compensaciones o penalizaciones* que se efectuarán al cliente cloud en el caso de que el proveedor y/o sus subcontratistas *incumplan sus obligaciones contractuales derivadas PLA*, así como las compensaciones contractuales existentes en el caso de fallos en el cumplimiento de las estipulaciones sobre seguridad, monitorización, notificación de violaciones de la seguridad, portabilidad de datos y/o obligaciones de retención de datos.

1.2.3. Contratos de encargo de tratamiento según RGPD y LOPDGDD.

Después de haber mencionado los elementos y garantías contractuales que deberían incluir los SLA o PLA en lo referente a protección de datos según el GT29, la Comisión

Europea o el CSA, convendría poner nuestro punto de mira en el legislador comunitario europeo y nacional y la nueva normativa que afecta también, a los servicios cloud (clientes como responsables y proveedores como encargados de tratamiento).

El art 28.3 RGPD señala concretamente las obligaciones del encargado (aplicables a los proveedores cloud):

> a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;

Se deberá "documentar de forma precisa las instrucciones respecto del encargo realizado" siendo "necesario identificar de forma clara y concreta cuáles son los tratamientos de datos a realizar por el encargado del tratamiento, atendiendo al tipo de servicio prestado y a la forma de prestarlo" (AEPD, Guía Directrices elaboración contratos entre responsables y encargados, pág. 6)[368].

> b)garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;

"Hay que establecer la forma en que el encargado del tratamiento garantizará que las personas autorizadas para tratar datos personales se han comprometido, de forma expresa, a respetar la confidencialidad o, en su caso, si están sujetas a una obligación de confidencialidad de naturaleza estatutaria. El cumplimiento de esta obligación debe quedar documentado y a disposición del responsable del tratamiento". (AEPD, 6)

> c) tomará todas las medidas necesarias de conformidad con el artículo 32;

"Corresponde al responsable del tratamiento realizar la *evaluación de riesgos* para determinar las medidas de seguridad apropiadas para garantizar la seguridad de la información tratada y los derechos de las personas afectadas. Así mismo el encargado también debe *evaluar los posibles riesgos* derivados del tratamiento, teniendo en cuenta los medios utilizados (tecnologías, recursos etc.) y otras circunstancias que puedan

[368] AEPD. Directrices para la elaboración de contratos entre responsables y encargados del tratamiento. Recomendado de https://www.aepd.es/media/guias/guia-directrices-contratos.pdf. Págs 11 – 18.

incidir en la seguridad, como por ejemplo que el encargado lleve a cabo otros tratamientos" (AEPD, 7). A partir de ahí se podrá elaborar una *lista exhaustiva* de las mismas o remitir a un *estándar o marco nacional o internacional reconocido*. Además, teniendo en cuenta varios factores como indica el art. 32 (estado de la técnica, costes, naturaleza, riesgos, probabilidad…) tanto el responsable (cliente cloud) y el encargado del tratamiento (proveedor cloud) establecerán las *medidas técnicas y organizativas*.

> d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;

"El acuerdo debe establecer el régimen de subcontratación. El RGPD exige la autorización previa por escrito del responsable del tratamiento para que el encargado del tratamiento pueda recurrir a otro encargado (subencargado)" (AEPD, 8).

> e) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;

"Hay que establecer la forma en la que el encargado del tratamiento asistirá al responsable en el cumplimento de la obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados[369]" (AEPD,8)

> f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

"Se debe establecer la forma en que el encargado ayudará al responsable a garantizar el cumplimiento de las obligaciones relativas a la aplicación de las medidas de seguridad que correspondan, la notificación de violaciones de datos a las Autoridades de Protección de Datos, la comunicación de violaciones de datos a los interesados, la realización de las evaluaciones de impacto relativa la protección de datos y, en su caso, la realización de consultas previas". (AEPD, 9)

[369] "En cuanto al derecho de información de las personas afectadas, se trata de un derecho no sujeto a solicitud y, por tanto, no sujeto a las previsiones del artículo 28.3.e) del RGPD. Pese a ello, en aquellos casos en que el encargado deba realizar la recogida de datos es recomendable establecer en el acuerdo o acto jurídico la forma y el momento en que debe darse el derecho de información" (AEPD, 8).

> g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;

"El acuerdo debe establecer de forma clara cuál de las dos opciones es la elegida por el responsable, así como la forma y el plazo en que debe cumplirse. En todo caso, los datos *deberán ser devueltos al responsable* cuando se requiera la conservación de los datos personales, en virtud *del Derecho de la Unión o de los Estados miembros*. No obstante, el encargado puede conservar una copia con los datos *debidamente bloqueados*, mientras puedan derivarse responsabilidades de la ejecución de la prestación". (AEPD, 9)

> h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

Ahora bien, habiendo señalado el contenido mínimo y pudiendo recurrir a las plantillas de modelos de contratos puestos a disposición de la AEPD en la guía citada, convendría aclarar una cuestión importante que muchos nos preguntábamos antes incluso de la entrada en vigor del propio RGPD, me refiero al estado o situación de los contratos de encargo cloud suscritos anteriormente al 25 de mayo de 2018. La respuesta nos la ha dado el legislador nacional en la LOPDGDD (disposición transitoria quinta). El legislador señala que estos contratos (también de encargo cloud) mantendrán su vigencia hasta el 25 de mayo de 2022 hasta la fecha de vencimiento señalada en los mismo y en caso de que se hayan pactado de forma indefinida. Durante ese plazo, cualquiera de las partes podrá "exigir" a la otra la modificación del contrato a fin que el mismo resulte conforme al citado art. 28.3. RGPD.

1.3. **Transferencias internacionales y ("BCR")**

El uso de *cloud* implica, por regla general, el trasiego internacional de datos, bien porque el proveedor *cloud* esté en terceros países, o bien porque, lo más frecuente en *cloud* es la subcontratación de servicios por los proveedores. No todas las regulaciones de protección de datos en el mundo son tan exigentes como la europea lo que puede derivar a una reducción del nivel de exigencia local si los datos salen. La solución no

estaría tanto en bloquear los datos personales hacia el exterior (puesto que todas las economías necesitan transmitir datos hacia el exterior) sino subir el nivel de adecuación de los terceros países.

A continuación tenemos un ejemplo de servidor *cloud hosting* con posibilidad de elegir el país donde alojar los datos en cloud.

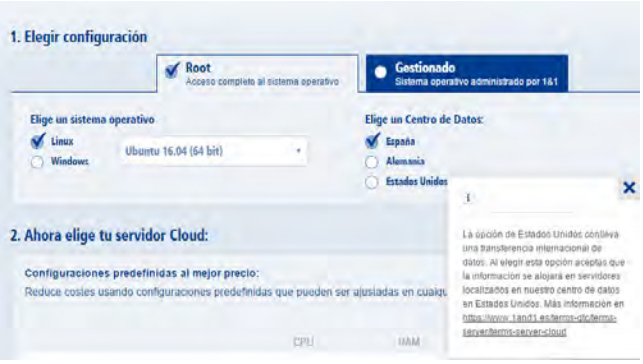


Imagen 42. Fuente: 1&1. Ejemplo de servidor hosting cloud con data center con posibilidad de elegir entre España, Alemania o EEUU[370].

La naturaleza de esta tecnología permite cierta "flexibilidad" como si se tratara de un "traje a medida" para cada cliente. Por tanto el *proveedor* podrá decidir dónde o en qué servidores podrá tratar los datos de los que será encargado[371]. En el terreno legal, un lugar físico significa *jurisdicción* por lo que se suele recomendar que se consulte a los proveedores cuál es su jurisdicción y marco regulatorio en materia de protección de datos. En verdad, la realidad es que los proveedores no ofrecen la información sobre la geolocalización de sus *data center*, y lo que es más grave, hay proveedores que incluso ofrecen descuentos si se permite al proveedor que elija en cada momento donde residenciar los servicios cloud contratados[372].

Además es de tener muy en cuenta que una transferencia internacional de datos se produce como *"conditio sine qua non"* y eso implica que el cliente cloud se convierte automáticamente en responsable del tratamiento, de ahí la importancia que tiene el conocimiento efectivo de la geolocalización de los data center.

[370] Vid. https://www.1and1.es/servidor-cloud-dinamico#configuracion-del-servidor

[371] A la hora de elegir la ubicación del data center se recomienda a grandes rasgos que se escoja zonas de baja sismicidad, con infraestructuras adecuadas, inundables, climatológicamente adecuadas (aunque *eBay* tiene un data center en el desierto), evitar lugares cercanos a vías ferroviarias…etc.

[372] En la política de privacidad de Amazon se puede leer: "Puede especificar las regiones AWS en las que se almacenará . No moveremos su contenido de su AWS seleccionado regiones sin notificarle, a menos que sea necesario para cumplir con la ley o las solicitudes de entidades gubernamentales".

Tal y como menciona *Alamillo Domingo*[373], citando al NIST, " la localización física de los datos entregados por el proveedor de servicios en el Cloud es una de las funciones pendientes de solución satisfactoria, en especial atendiendo a la necesidad de cumplimiento de las leyes y regulaciones que priva el almacenamiento o el procesamiento transfronterizo de datos, si bien en sus recomendaciones, para el uso del Cloud figura claramente la regulación por vía de contrato negociado de la obligación del proveedor de mantener los datos del territorio o territorios indicados por la administración". Según este autor, la amenaza principal relacionada con la deslocalización de los datos deriva de:

> a). "En primer lugar, los otros podrían encontrarse en una jurisdicción donde la legislación no protege adecuadamente los datos. En este caso datos de carácter personal.
>
> b). En segundo lugar, la ubicación de los datos en una localización concreta podría suponer la infracción de la legislación, bien referida obligaciones en el país de origen, bien por constituir una infracción en el país de destino (o de tránsito o ubicación temporal, cuando la ley resulte aplicable a dichos casos) de los datos.
>
> c). En tercer lugar, los datos podrían encontrarse en una jurisdicción donde no resulta posible impedir actividades infractoras similares en relación con la tos, su propietario o terceros".

CloudCarib es un ejemplo de proveedores de servicios *cloud offshored* (deslocalizados) dirigido a clientes con información sensible que huyen de la legislación estadounidense.

Imagen 43. Ejemplo de proveedor off-shored. Fuente: CloudCarib[374].

Lo que es claro es que dado el auge de este mercado, la ubicación de los data center de *"Cloud Computing"* tienen claras consecuencias económicas. Curiosamente, los proveedores cloud que están emergiendo son aquellos que tienen *data center* en latitudes frías, donde el coste de refrigeración de los servidores es muy bajo. Esto

[373]Vid. ALAMILLO DOMINGO, Ignacio. Obra Citada, donde a su vez se cita al NIST 2011
[374] Vid. http://www.cloudcarib.com/

contribuye a que los datos gestionados por el proveedor de cloud computing puedan tener múltiples ubicaciones a lo largo de la vigencia del contrato. Si las oscilaciones en los precios del hosting son importantes, el proveedor de cloud computing podría cambiar la ubicación de los datos con una mayor frecuencia.

1.3.1. Transferencia internacional: concepto y novedades en RGPD.

El legislador en el RGPD no aporta definición a este concepto[375] sino únicamente elabora una definición "abierta" de lo que es un tratamiento transfronterizo. Antes del RGPD, el legislador comunitario estableció que el exportador[376] de datos podía ser tanto responsable como encargado del tratamiento, lo que daba lugar a que los proveedores de servicios cloud establecidos en terceros países se encontrasen en mejor situación a la hora de subcontratar en esos u otros terceros países que los prestadores de servicios establecidos en la UE. Anteriormente con la Directiva, se obligaba a los exportadores a solicitar autorización previa para poder transferir datos a importadores establecidos en países que no contaban con un nivel adecuado de protección, siempre que aporten las *garantías suficientes*[377], y a notificar las transferencias cuando se dirigen a países que sí disponen de dicho nivel adecuado.

---

[375]La definición más acertada de "transferencia internacional" la encontrábamos en el antiguo Reglamento de desarrollo LOPD en su artículo 5.1.s) como *"el tratamiento que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español"*. Es decir, se produciría cuando constituya una cesión o comunicación de datos o cuando tenga por objeto la realización de un tratamiento de datos por cuenta del responsable. En ambos supuestos se produce una salida física de datos fuera del EEE. Pero en el caso de acceso a los datos por cuenta de un encargado del tratamiento no se produce una salida jurídica de los datos, ya que el responsable del tratamiento está establecido en el territorio español y la norma que continuará aplicándose será la española.

[376] El antiguo Reglamento de desarrollo de LOPD definía en su artículo 5.j) "e*xportador de datos personales*" a la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.

[377] SEPD (2012) Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe". Recuperado de https://edps.europa.eu/sites/edp/files/publication/12-11-16_cloud_computing_en.pdf. El SEPD (2012), ya estableció como medidas recomendadas en el contexto de las transferencias internacionales: (i) clarificar y proporcionar orientación sobre la forma de garantizar la eficacia de las *medidas* de protección de datos en la práctica y apoyar el uso de normas corporativas vinculantes por parte de los proveedores de servicios; (ii) promover el desarrollo de las *mejores prácticas* en temas como la responsabilidad responsable/encargado, la retención de datos en el entorno de la nube, la portabilidad de datos y el ejercicio de los derechos de los interesados; (iii) elaborar normas de desarrollo y sistemas de *certificación* que incorporen plenamente los criterios de protección de datos; (iv) *definir claramente la noción de transferencia* y los criterios bajo los cuales se podría acceder a los datos en la nube por los organismos encargados de hacer cumplir la ley fuera de los países del EEE.

Con la llegada del RGPD, aparecen las novedades en torno al régimen de *autorización y notificación previa* de las transferencias internacionales que quedan reducidas a muy pocos supuestos. Ahora, con carácter general, las transferencias se pueden llevar a cabo sin necesidad de autorización previa, salvo que las garantías se aporten a través de un *contrato entre el responsable o el encargado del tratamiento*, encargado o destinatario de los datos personales en el tercer país u organización internacional, o de un *acuerdo administrativo* entre autoridades públicas, supuestos en los que será preciso que exista la autorización de la autoridad de control, tal y como señala el artículo 46.3 del RGPD.

Por su parte, en el artículo 46.2 del RGPD se relacionan las *garantías adecuadas*[378][379] que podrán ser aportadas *sin que se requiera ninguna autorización expresa* de una autoridad de control. Las garantías podrán ser instrumentos jurídicamente vinculantes y exigibles entre las autoridades u organismos públicos, un mecanismo de certificación, las cláusulas tipo de protección de datos adoptadas por la Comisión, cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión, un código de conducta o las normas corporativas vinculantes ("BCR").

El Reglamento establece que a falta de los instrumentos anteriores, se podrá realizar transferencias de datos a países sin un nivel adecuado de protección si se cumplen alguno de los requisitos que marca el legislador en el art. 49.1 RGPD[380]. Uno de los requisitos es el contar con el propio consentimiento (art. 49.1.a) "reforzado"[381]:

> **"**el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, *tras haber sido informado* de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas".

[378] En todo caso, esas garantías adecuadas que el responsable o el encargado del tratamiento *deberán tomar medidas para compensar la falta de protección de datos* en un tercer país mediante garantías adecuadas para el interesado estarán referidas al cumplimiento de los *principios generales* relativos al tratamiento de los datos personales y los principios de la protección de datos desde el diseño y por defecto, y a poner a disposición de los interesados sus *derechos exigibles y de acciones legales efectivas*, incluyendo el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización, en la Unión o en un tercer país.

[379] El SEPD ya en el 2012 en su Dictamen de 7 de marzo consideraba oportuno "sustituir o aclarar la referencia a las «garantías adecuadas» del artículo 44, apartado 1, letra h)".

[380] Esto significa que basta con cumplir uno de los requisitos.

[381] En este sentido habría que asegurarse de que entienden todos y cada uno de los riesgos que suponen. como el abogado J. Campanillas (2016), señaló ; "debemos entender que no valdrá un simple párrafo, como sucede en la actualidad, donde se otorga un consentimiento para una cesión, sino que deberá ser más detallada la información a otorgar al afectado e incluso, diría yo, un posible *check box* para que podamos probar dicho consentimiento explícito con los riesgos que conlleva la transferencia"

Pero no solo el consentimiento, también se otorgan otras posibilidades como son que; la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento *o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado; la transferencia sea necesaria para la* celebración o ejecución de un contrato, en interés del interesado*, entre el responsable del tratamiento y otra persona física o jurídica; la transferencia sea necesaria por* ***r***azones importantes de interés público***;*** *la transferencia sea necesaria para la* formulación, el ejercicio o la defensa de reclamaciones**.**

Por último, en el apartado 2 del art. 49, se abre otra vía como posible cajón desastre cuando no encontramos un encuadre en ningún de las opciones establecidas, introduce la figura de los "intereses legítimos imperiosos**".**

Ahora bien, cuando una transferencia no pueda basarse en disposiciones de los artículos 45 o 46, incluidas las disposiciones sobre normas corporativas vinculantes, **y** *no sea aplicable ninguna de las excepciones* para situaciones específicas a que se refiere el párrafo primero del presente apartado, solo se podrá llevar a cabo si no es repetitiva**,** afecta solo a un número limitado de interesados**,** es necesaria a los fines de *intereses legítimos imperiosos* perseguido**s** por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales.

1.3.2. Normas corporativas vinculantes ("BCR") y RGPD.

Son el instrumento más adecuado para regular las transferencias internacionales de datos en los grupos multinacionales, sin embargo los plazos para su aprobación por las autoridades en materia de protección de datos, la complejidad del proceso y los costes elevados han hecho que muchos grupos no se las planteen como una solución viable. Están dedicadas a las *transferencias no repetitivas*[382] que afecten a un número limitado de interesados.

[382] El SEPD, ya opinó en su Dictamen de 7 de marzo de 2012 que en el artículo 44 se debería *"añadir que la posibilidad de transferir datos debería afectar únicamente a las transferencias ocasionales y que debería estar basada en una evaluación cuidadosa, caso por caso, de todas las circunstancias de la transferencia".* También cree oportuno "sustituir o aclarar la referencia a las «garantías adecuadas» del artículo 44, apartado 1, letra h)".

2. REGIMEN JURÍDICO APLICABLE AL USO DE IOT DE LA SALUD.

2.1. La importancia de la seguridad en la privacidad en IoT.

El art. 32.1 del Reglamento europeo señala que;

> "Teniendo en cuenta el *estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto*[383] y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al *riesgo*[384] (…)"

El experto Pedro Alberto, de la Agencia Vasca de Protección de Datos[385], (2015) señaló acertadamente una distinción necesaria entre seguridad y privacidad. Distingue a la seguridad - *adjetivo*- como un medio para proteger a los activos -evitando riesgo y mitigando impacto- a diferencia de la privacidad –*sustantivo*- como un fin y un derecho fundamental constitucional. Partiendo de esa base, focalicemos nuestra atención en los problemas que despierta la seguridad de la que estamos hablando y de posibles soluciones según el GT29 en su Dictamen del 2015[386].

i. La IoT implica una compleja cadena de suministro con múltiples partes interesadas asumiendo *diferentes grados de responsabilidad***.**
ii. Adicionalmente, *la ausencia de actualizaciones automáticas* revierte en la existencia de vulnerabilidades frecuentes.

---

[383] Partimos de la base de que las medidas de seguridad se llevarán a cabo teniendo en cuenta las limitaciones operativas específicas de los dispositivos IoT. Por ejemplo, hoy en día, la mayoría de los sensores no son capaces de establecer un vínculo cifrado debido al prioridad que se da a la autonomía física del dispositivo o al *control de costes*.

[384] Los analistas de la compañía de ciberseguridad *Kaspersky Lab* ya alertaron hace un par de años del alto nivel de desprotección de la información médica y de los datos de los pacientes almacenados en la infraestructura sanitaria conectada. También señalaban algo importante: los datos eran muy atractivos para el mercado negro y podrían ser de interés no sólo para ciberdelincuentes sino para compañías aseguradoras, interesadas en saber cómo podría llegar a afectar a las primas o a la seguridad laboral. Ocurrirá igual a la información transmitida entre los wearables, incluidos implantes, y los profesionales del sector sanitario.

[385] González, P.A. (2015). Privacidad en la Internet de las Cosas. Recuperado de https://www.slideshare.net/pagonzalez/privacidad-en-la-internet-de-las-cosas-presentacin

[386] GT29. Opinion 8/2014 on Recent Developments on the Internet of Things. (WP 223). Recuperado de https://www.dataprotection.ro/servlet/ViewDocument?id=1088

iii. Algunos de los sistemas de comprobación automática (por ejemplo, seguidores del sueño), sufren *fallos de seguridad* que permiten a los atacantes manipular los valores.

Algunas soluciones las podemos encontrar en la normativa existente:

i. Las *evaluaciones* de seguridad de los sistemas. Incluyendo la seguridad de los componentes. Piénsese en posibles certificaciones de dispositivos, el uso de estándares internacionales de seguridad en IoT.
ii. *La privacidad desde el diseño (o seguridad desde el diseño).* Piénsese en la desactivación por defecto de funcionalidades no críticas, la prevención del uso de fuentes de actualización de software no sean de confianza.
iii. El principio de *minimización* de los datos. Esto implica restringir el tratamiento de datos personales, incluyendo recogida, almacenamiento, etc (Ver art. 4.2. RGPD).

2.2. Los sujetos jurídicos implicados

De igual modo, todos los actores deberán prestar especial atención a que los datos de salud son *datos de categoría especial* (art. 9.1 RGPD) .

2.2.1. Titulares de los datos personales

Son aquellas personas afectadas o interesadas que entregan información sensible que les de forma consentida o no, mediantes las aplicaciones IoT a los proveedores de las mismas, en las cuales se realizarán algún tipo de tratamiento de datos personales. A continuación, trataremos algunas cuestiones de interés. En primer lugar, podríamos pensar que si las personas físicas utilizan dispositivos IoT para su propio uso con fin personal se podría encuadran en tratamientos de datos "domésticos"[387] -donde no hay conexión con actividades comerciales o profesionales- y a su exención (art. 2.2.c RGPD) en la aplicación de la normativa. Sin embargo, en la práctica, el modelo de negocio implica que los *datos del usuario*[388] se transfieren de forma automática a los *fabricantes de dispositivos*, *desarrolladores de aplicaciones*[389] y otros terceros.

[387] Vid. https://www.clarin.com/sociedad/lentes-inteligentes-ciegos-realidad-venden-varios-paises_0_HyxEvbOHb.html

[388] Según la consultora *Kaspersky*, a finales de 2016, los routers domésticos de un proveedor telecomunicaciones europeo eran atacado por el gusano Mirai. Después de que analizaran este incidente llegaron a la conclusión de que los usuarios no tenían conocimiento de que sus aparatos domésticos habían sido comprometidos y formaban parte de un enorme botnet. Tampoco sabían de la actividad de red

En segundo lugar, se podrá incluir como tratamiento de datos en la IoT también cuando afecte a personas diferentes a los propios usuarios de esa IoT. Piénsese, en el caso *gafas inteligentes para control de personas*[390]las cuales tienen capacidad para recoger datos personales como datos biométricos. Estos casos también son objeto de aplicación encuadrados en el RGPD. En tercer lugar y respecto a los derechos de los titulares (tanto usuarios como personas afectadas), la partes involucradas deberán cumplir con el cap. III del RGPD. Respecto a la legitimación del tratamiento si se opta por el consentimiento, se recuerda que este deberá ser *libre, informado, específico e inequívoco*, no pudiéndose deducir del silencio o de la inacción de las personas.

---

de sus dispositivos conectados como televisores, monitores de bebés, lavadoras, etc. Ver https://os.kaspersky.com/wp-content/uploads/sites/11/2018/04/Kaspersky-IoT-security-whitepaper_print.pdf

[389] AEPD- UPM (2019) *Análisis de flujos de información en Android. Herramientas para el cumplimiento de responsabilidad proactiva*. Recuperado de https://www.aepd.es/media/estudios/estudio-flujos-informacion-android.pdf .

Señala concretamente que :"Las aplicaciones en los teléfonos móviles pueden manejar datos como las fotografías, correos o la agenda de actividades, pueden acceder a ciertos datos generados por sensores integrados en el dispositivo o conectados a él, como la localización o los signos vitales de los usuarios. El responsable del tratamiento realizado por una aplicación móvil tiene la obligación de informar al usuario a través políticas de privacidad, notificaciones o descripciones publicadas en las tiendas de aplicaciones, y la implementación efectiva del servicio ha de ajustarse a los límites de esa información, de la legitimación para el tratamiento y las garantías generales del RGPD. La realidad es que *el responsable del tratamiento de los datos de una app no siempre será el desarrollador directo y exclusivo de esta, se basará en librerías de terceros, subcontrataciones o acuerdos y/o en la ejecución en el entorno de un tercero*, por lo que hay una potencial pérdida de control sobre la implementación de dicho tratamiento y un aumento de la complejidad para abordar los mencionados requisitos de cumplimiento en materia de protección de datos. Los desarrolladores de aplicaciones móviles, los responsables que subcontraten dichos desarrollos y distribuidores o repositorios de apps *tienen la obligación de asegurar que las apps que ponen a disposición de los usuarios están de acuerdo a las políticas de privacidad y los servicios publicitados con las garantías adecuadas (principio de responsabilidad proactiva)*.

[390]Vid. https://www.xataka.com/wearables/estas-gafas-inteligentes-toshiba-dynaedge-dispositivo-reconocimiento-facial-basado-windows

Conceptos previos.

"Tratamiento de datos" es "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción" (Art. 4.2. RGPD).

"Dato personal" es "toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha personal" (Art. 4.1. RGPD).

"Datos biométricos" son "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos" (Art. 4.14 RGPD)

"Datos relativos a la salud" son "datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud" (Art. 4.15 RGPD).

Además, tendrán la *posibilidad de revocar o retirar el consentimiento previo*[391] dado al tratamiento de información específica y de oponerse al tratamiento. Además, el ejercicio de los derechos (cap.III) se deberá realizar sin restricciones o impedimentos técnicos u organizativos, y las herramientas proporcionadas para registrar esta *retirada*[392] deben ser accesibles, visibles y eficaces. Esto es bastante determinante teniendo en cuenta la naturaleza de esta tecnología.

En cuarto lugar y respecto al derecho de acceso existen ciertas particularidades sobre todo en lo referente a los datos en bruto. A pesar de no despertar un gran interés a los titulares serían de gran utilidad para realizar migración de los datos personales (por

[391] Según GT29 (2015,7), algunos desarrolladores dan un mayor control sobre las funciones de administración del consentimiento, por ejemplo, mediante el uso de *sticky-policies* o *privacy proxies.* Sin duda, la utilización de estos funciones estarían encuadras en el principio de responsabilidad proactiva por parte de los que vayan a ser responsables de tratamiento de datos en IoT.

[392] El GT29 (2015, 29) señaló algo muy interesante; los esquemas de retirada deberán de ser "*de grano fino*" donde deberían incluirse el objeto específico, el tipo de dato específico y el tratamiento específico. (Por ejemplo, el titular de los datos debería ser capaz de solicitar que se deje de recoger datos biométricos, que deje de recoger datos de seguimiento del sueño y que el dispositivo en cuestión dejara de hacer seguimiento de los pasos.)

ejemplo, si *FITbit* cambia la política de privacidad). El GT29 en su dictamen señala que si no se permite el acceso a esos datos se impedirá el ejercicio efectivo del derecho de acceso (art. 15 RGPD), en consecuencia, el derecho a la portabilidad (art. 20 RGPD). Los proveedores de IoT "lock-in" tendrían los días contados con la llegada de la nueva normativa y el nuevo derecho a la portabilidad. Con ello, el legislador pretendió desbloquear los obstáculos de competencia.

2.2.2. Fabricantes de dispositivos IoT

Algunos ejemplos pueden ser Fitbit, Google Health, Apple (Healthkit, Apple Watch), Samsung (S Health). En muchos casos, éstos y los equipos de telecomunicaciones ignoran los principios fundamentales de la seguridad[393].

Según el GT29 (2015,14) , los fabricantes de dispositivos en la IoT no solo venden artículos físicos a sus clientes o productos de marca blanca a otras organizaciones sino que también pueden haber desarrollado o modificado el sistema operativo del "objeto" o un programa que garantice su funcionalidad en general, incluidos los datos y la frecuencia de recogida, el cuándo y a quién se transmiten los datos, y con qué efectos. En concreto, señala un ejemplo llamativo en materia de prevención de riesgos laborales pero que es una realidad en EEUU[394]; "las empresas podrían fijar el precio del seguro de sus empleados basándose en los datos (de salud) reportados por dispositivos *wearables* seguidores de lo que hacen". Las aseguradoras, no sólo estadounidenses sino también españolas[395], han visto en IoT un instrumento para rentatibilizar el negocio o para ofrecer sus servicios con primas de seguro más bajas.

---

[393] Según *Kaspersky*, "el hardware no controla el integridad del firmware, los dispositivos se envían con contraseñas preinstaladas, incluyendo sin mencionar las débiles configuraciones de seguridad de la red o el uso de las contraseñas de de versiones de software antiguas y vulnerables. Además, un proceso de actualización de software no es siempre se proporcionan, lo que significa que los dispositivos vulnerables pueden funcionar durante años sin actualizaciones. Es sólo cuestión de tiempo antes de que estos dispositivos sean atacados con éxito".

[394] Ver en https://communityofinsurance.es/blog/2017/11/19/asi-impacta-el-internet-de-las-cosas-en-el-sector-asegurado/ y https://newsroom.uhc.com/. (En EEUU existen compañías como ***UnitedHealthcare*** cuyos clientes llevan una pulsera que monitoriza su ejercicio diario: número de pasos, intensidad y consistencia. Si el cliente cumple unos determinados objetivos, obtienen una bajada en su prima anual del seguro de salud – desde 4 dólares diarios hasta 1.460 dólares mensuales – puesto que se supone que disminuye el riesgo de sufrir ciertas enfermedades asociadas a la falta de actividad física").

[395] Vid. https://www.inithealth.com/en/

Fuente Revista APD. Enero/febrero 2019. Empresa Inithealth

Hay que tener en cuenta algunas obviedades (o no tanto) que señala el GT29 como que los fabricantes deberán; (i) informar del tipo de datos que son recogidos por los sensores y los que se tratarán después y cómo; (ii) ser capaces de hacer llegar a todos los demás actores involucrados cuando un interesado retira su consentimiento o se opone al tratamiento de datos; (iii) proporcionar *opciones granulares* (tipo, tiempo y frecuencia de recogida) en la concesión de acceso a las aplicaciones[396]; (iv) proporcionar herramientas para leer localmente, editar y modificar los datos antes de ser transferidos a cualquier responsable del tratamiento; (v) proporcionar un interfaz fácil de usar para los usuarios que quieren obtener tanto los datos agregados y/o los *datos en bruto*; (vi) proporcionar herramientas fáciles para notificar vulnerabilidades de seguridad; (vii) limitar tanto como sea posible la cantidad de datos almacenados en los dispositivos mediante la transformación de los datos en bruto en los datos agregados directamente en el dispositivo.

2.2.3. Desarrolladores de API[397]

[396] En este sentido, el GT29 señala que de manera similar a la característica de "no molestar" en los teléfonos inteligentes, los dispositivos IoT deberían ofrecer una opción de "no recogen" para programar o desactivar rápidamente sensores. Para evitar el seguimiento de localización, los fabricantes de dispositivos deben limitar la huella dactilar del dispositivo mediante la desactivación de las interfaces inalámbricas cuando no se utilicen o deban utilizar identificadores aleatorios (como direcciones MAC aleatorias para escanear redes wifi) para evitar un identificador persistente de sea utilizado para el seguimiento de la ubicación.

[397] API es el acrónimo inglés “Application Programming Interface”, es decir, “Interfaz de Programación de Aplicaciones”. Una “interfaz” es la forma en que dos aplicaciones o servicios se comunicar entre sí. Lo hacen exponiendo al resto de aplicaciones el conjunto de servicios disponibles en cada una y cómo se deben acceder.

Medicare o Medicaid[398] con la Api Blue Bottom 2.0[399]) que permite a los beneficiarios de Medicare conectar sus datos de reclamaciones a las aplicaciones, servicios y programas de investigación en los que confían.

Otras son MuleSoft, Practo Technologies, Microsoft, Allscripts Healthcare, General Electric, Greenway Health, eClinicalWorks, Practice Fusion y Apple[400].

Tal y como establece el GT29, muchos sensores proporcionan API para facilitar el desarrollo de aplicaciones y esto a menudo consiste en proporcionar al desarrollador de la aplicación un *acceso a los datos* a través de la API[401]. Y "a menos que estos datos sean completamente anónimos, tal acceso constituye una *transformación*, por lo que el desarrollador de la aplicación que ha decidido este acceso a los datos debe ser considerado como un *responsable del tratamiento* en virtud de la legislación comunitaria"[402]. El deber de información (art. 13 RGPD) debe ser continuo a través de avisos o envíos a email para recordar que se están extrayendo datos. Además, deberán tener presente el principio de minimización y sin acceder a los datos en bruto y la privacidad desde el diseño.

2.2.4. Organizaciones de la Industria del cuidado de la salud o aseguradoras de salud (responsables)

Los terceros que no sean los fabricantes de dispositivos ni desarrolladores de aplicaciones pueden utilizar dispositivos IoT para *recoger y procesar información sobre los individuos*.

Por ejemplo, *laboratorios farmacéuticos* como responsables del tratamiento pueden encargar a desarrolladores que diseñen una API para crear una app (como Social Diabetes) y que tendrán obligaciones de encargado de tratamiento. A su vez, el desarrollador de API, podrá subcontratar a otros desarrolladores o proveedores como redes sociales (por poner un ejemplo).

---

[398] Vid. https://www.ca.com/en/blog-highlight/apis-for-your-ehr.html

[399] Vid. https://bluebutton.cms.gov/

[400] Vid. https://www.transparencymarketresearch.com/healthcare-api-market.html

[401] Algunas aplicaciones pueden recompensar a los usuarios de objetos concretos, por ejemplo, una aplicación desarrollada por una *compañía de seguros de salud* podría recompensar a los usuarios de "objetos" de cuantificación automática. Para más info véase: https://clipset.20minutos.es/una-aseguradora-quiere-implantar-el-apple-watch-como-regalo-para-sus-clientes/

[402] Dichas aplicaciones se instalan tradicionalmente en base al opt-in donde en puede que esté sometido al consentimiento pero no siempre en las solicitudes está contenida suficiente información para considerar al consentimiento como específico y suficiente.

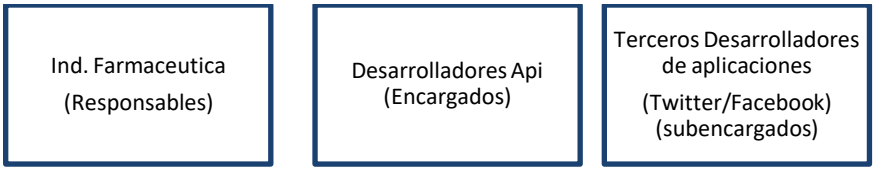


Imagen 43. Ejemplo de cadena de suministro en IoT y la Industria del Cuidado de la Salud.

Por otro lado, los *seguros de salud* pueden desear dar una pulsera wearable[403] para sus clientes y así controlar la frecuencia con que realizan ejercicio y adaptar sus primas de seguro en consecuencia. Pero, ¿en qué se diferencian de los fabricantes? En que estos no tienen control sobre el tipo de datos recogidos, pero sí serían considerados como *responsables del tratamiento* para el proceso concreto de esos datos, en la medida en que recogen y almacenan los datos generados por estos dispositivos IoT para fines específicos que han decidido ellos mismos. Los suscriptores son titulares de datos y deberán tener acceso a su cuenta en la aplicación del seguimiento de pasos.

2.2.4. Plataformas de datos

"Los fabricantes han desarrollado progresivamente plataformas que tienen como objetivo *alojar los datos recogidos* a través de este tipo de dispositivos diferentes, con el fin de centralizar y simplificar su gestión" (GT29). Estas plataformas se podrán calificar como *responsables del tratamiento*, cuando el desarrollo de este tipo de servicios implique una recogida de datos personales de los usuarios *para sus propios fines*.

Una plataforma de datos puede estar formada por datos provenientes de muchas aplicaciones, por ejemplo, la plataforma de datos mundial de diabetes en la que participa la aplicación Social Diabetes formada por centros, clínicas, médicos, pacientes.

2.2.5. Las plataformas sociales

El GT29 no va mal desencaminado cuando indica que "los interesados son aún más propensos a hacer uso de las cosas conectadas cuando pueden compartir esos datos públicamente o con otros usuarios" como por ejemplo, las propias redes sociales[404]. Este es un ejemplo de la aplicación española *Social Diabetes* en el momento de la

[403] Vid. https://blog.puntoseguro.com/reto-puntoseguro-seguros-que-te-recompensan-por-estar-sano/ y https://www.puntoseguro.com/seguros-de-vida/

[404] El GT29, señala un ejemplo, una red social puede utilizar la información recopilada por un podómetro para inferir que un usuario en particular es un corredor regular y muestra sus anuncios sobre los zapatos para correr.

inscripción y en el momento que un usuario con diabetes publica su información personal en la red social de Twitear incluyendo fotografía, nombre y apellidos (cuya información es susceptible de ser indexada en las redes sociales)

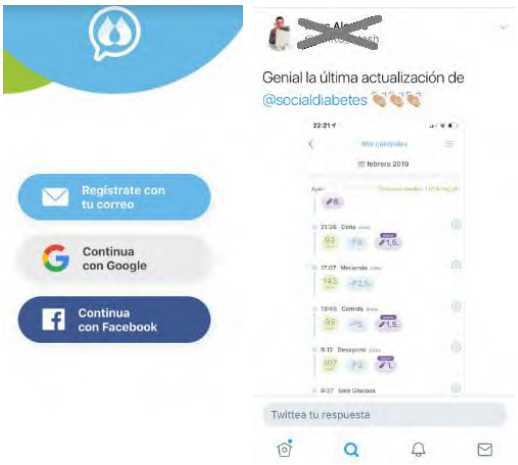


Imagen 44. Pantallazo de situación de riesgo para titular de datos y usuario de app Social Diabetes.

Aquí hay un problema: el usuario sube un informe con los resultados - donde éstas tratan estos datos para fines distintos de los que habían autorizado- convirtiéndose el usuario en el responsable junto con la red social. Es decir, a mi parecer, el GT29 se referiría a la co-responsabilidad del art. 36.1 RGPD[405] que establece;

> "cuando dos o más responsables *determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento*. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos. Dicho acuerdo podrá designar un punto de contacto para los interesados".

El GT29, detalla que "las consecuencias de esta calificación se han detallado en el *Dictamen WP9 sobre redes sociales"* [406][407].

[406] Opinion 5/2009 on online social networking adopted on 12 June 2009 (WP 163). Recuperado de http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf

[407] En todo caso, el titular de los datos debería poder especificar en las aplicaciones sociales (RRSS) que se le solicite autorización y se le posibilite editar la información personal antes de publicar en las mismas.

2.2.6. Dueños dispositivos IoT

Podemos ser nosotros mismos como usuarios de eHealth y de dispositivos móviles para el seguimiento de una enfermedad como es la diabetes.

CAPÍTULO IV. RÉGIMEN JURIDICO EN PROTECCIÓN DE DATOS DE BLOCKHAIN/DLT DESDE EL ENFOQUE DE LA INDUSTRIA DEL CUIDADO DE SALUD DIGITAL

SUMARIO: 1. INTRODUCCIÓN.- 2. PARTICULARIEDADES JURÍDICAS GENERALES DE PROTECCIÓN DE DATOS EN BLOCKCHAIN Y DLT. 2.1. Los sistemas de gestión de identidad aplicables a blockchain. 2.2. Los contratos inteligentes. 2.3. Blockchain como herramienta de compliance. 3. PARTICULARIEDADES JURÍDICAS GENERALES DE PROTECCIÓN DE DATOS EN BLOCKCHAIN Y DLT. 3.1. El tratamiento de datos personales y el consentimiento en blockchain. 3.2. El concepto de "dato personal" en blockchain. 3.3. Tipos de datos en blockchain y DLT. 3.4. Los sujetos jurídicos en el tratamiento en blockchain. 3.5. Obligaciones de los sujetos jurídicos. 3.6. Respecto a la privacy by design/default. 4. INCOMPATIBILIDADES CON RGPD Y APROXIMACIÓN A POSIBLES SOLUCIONES. 4.1. Respecto a la transparencia y la designación del responsable. 4.2.Respecto al principio de minimización de datos personales. 4.3.Respecto al derecho de rectificación. 4.4.Respecto al derecho de acceso 4.5.Respecto al derecho de supresión (o al olvido) 4.6.Aproximación a soluciones: Off chain y side chain 4.7.Aproximación a soluciones: Uso de IA de middleware. 4.8.Respecto a la limitación del plazo de conservación. 4.9. Respecto al equilibrio innovación tecnológica vs regulación.

"La imaginación es más importante que el conocimiento"

(Albert Einstein)

1. INTRODUCCIÓN

El Parlamento Europeo reconoció a finales de 2018 la necesidad de Blockchain en el comercio, pidiendo medidas para aumentar la adopción de esta tecnología en el comercio y la administración con una *resolución*[408] mitigando el escepticismo y rechazo que existía a principios de año. El Parlamento también insta a la Comisión a establecer

[408]En dicha resolución resaltan que el método de utilizar esta tecnología tendría el objetivo de: "…los exportadores podrían cargar todos sus documentos en una solicitud de autoridad pública respaldada por Blockchain y demostrar su cumplimiento con el trato preferencial otorgado por un TLC". El parlamento también declara que la tecnología Blockchain tiene potencial para "proporcionar confianza en la procedencia" de los productos, permitiendo a las autoridades aduaneras obtener la información requerida para las declaraciones.

un grupo asesor sobre la tecnología y llevar a cabo investigaciones políticas sobre la tecnología. Además señaló que "la UE tiene la oportunidad de convertirse en un actor líder en el campo de la cadena de bloques y el comercio internacional, y debe ser un actor influyente en la configuración de su desarrollo a nivel mundial, junto con socios internacionales".

Desde que en el 2009 surge Blockchain, el interés por ésta no ha parado de aumentar, y así se evidencia en el hecho de que empresas, startups y administraciones públicas y gobiernos[409] de todo el mundo estén realizando elevadas y millonarias inversiones para desarrollarla y tomar posiciones privilegiadas en la que será la próxima revolución industrial: el internet del valor (Preukschat y Molero, 2017)[410]. El único límite que conocerá está tecnología estará en la propia imaginación del ser humano. Existen ya aplicaciones de *blockchain* en *trading* de mercancías, en seguros, deportes, en el control de votaciones, salud, petróleo, etc. Todas ellas tienen un elemento en común: la gestión eficiente y segura de un valor o activo, denominado *token*, en un entorno donde no hay confianza entre los actores que intervienen en el proceso. Ese *token* puede ser una moneda, un informe clínico, un seguro médico un voto, un documento del registro, etc.

Como consecuencia, el impacto de esta tecnología en el sector jurídico es innegable. A continuación, vamos a hablar de algunas consideraciones al respecto. Su implantación puede llegar a suponer un cambio sustancial en el ámbito económico y jurídico tanto en el derecho privado como en el público obligando a planteamientos de reforma en los sectores del ordenamiento a nivel internacional y nacional. A efectos prácticos, la cadena de bloques, proporciona un entorno seguro y confiable para realizar transacciones económicas disminuyendo costes. A pesar de las críticas que ha recibido esta tecnología debido a la facilidad de los ciberdelincuentes para aprovecharse de las debilidades, la seguridad intrínseca y la posibilidad de "discriminar" o "rechazar" el acceso a individuos supone una auténtica revolución para todos los sectores e

[409] Vid. https://www.coincrispy.com/2018/11/27/candidato-presidencial-nigeria-blockchain-mandato/
[410] Preulschat, A. (coord.); Kuchkovsky, C.; Gómez, G.; Diez, D.; Molero, Í.: (2017) *Blockchain: La revolución industrial de internet*. Pág. 15.

industrias. Se irán configurando negocios mixtos en entornos P2P sobre plataformas, de modo colaborativo, conectado y autónomo[411].

El hecho de que los ataques cibernéticos a los bloques de cadena sean menos probables que dentro de la Red, no significa que sean imposibles, por lo que los legisladores, deberán estar atentos, sobre todo los reguladores financieros como IOSCO y ESMA. Las *blockchain* internas, dentro de una organización, podrán economizar procesos internos de empresas e instituciones pero solo las grandes blockchain de uso masivo que conecten a grandes operadores y grupos de interés pueden hacer efectivo todo el potencial de la tecnología DLT (Ibañez, 2018, 19). Según este autor, las redes públicas o abiertas carecen en la práctica de posibilidades reales de control jurídico homogéneo pero las *blockchain* cerradas o restringidas. En cambio, las cerradas requerirán ciertamente de más esfuerzo regulatorio, y autorregulatorio donde se posibilita una negociación racional y actualizable de *normas de funcionamiento* como son los *protocolos de consenso* las cuales permitirán a los operadores jurídicos públicos ejercer sus labores de control. Pero también pueden existir otras normas de *funcionamiento interno o de gobierno* (tanto de la infraestructura informática como en las asociaciones o consorcios, como por ejemplo, políticas operativas técnicas o sistemas de identidad digital)[412].

Antes de empezar a analizar cuestiones jurídicas del *Blockchain* debemos hablar del concepto de la "tecnología de registros distribuidos" o "DLT", la cual permite a los usuarios grabar y almacenar permanente, simultánea y públicamente los datos introducidos compartidos entre un grupo de personas en distintas máquinas o servidores informáticos llamados nodos. De esta colectividad se deriva el nombre de "registro

[411] Vid. D'ASARO BIONDO, Information Technology (cap.15) en LARREY, P -editor-(2017). Connected world, From Automated work to virtual wars: The future by those who are shaping it. Portfolio Penguin House, Londres, 290 en IBAÑEZ JIMENEZ, J. Wenceslao (2018). *Blockchain: Primeras cuestiones en el ordenamiento español.* Editorial DYKINSON, pp 18.

[412] Un ejemplo de ello son las apps descentralizadas construidas para generar mercados seguros y de uno universal de identidad digital soberana o autónoma de disposición no autorizada o inconsentida para cualesquiera fines prohibidos Cuando la Administración publica intervenga en la producción de esos protocolos, las *blockchain* se convertirán en espacios controlados sin posibilidad o con poca probabilidad de fraude. El objetivo de estas normativas o control es eliminar los abusos de los operadores que pretenden vulnerar el orden público constitucional y reducir situaciones de conflictos de intereses donde pudiera existir abuso de posición dominante por parte de grupos monopolísticos o competidores desleales (IBAÑEZ, 2018, 21).

distribuido" o *"distributed ledger"*[413] debido a la dispersión de dichos nodos. Todo ello se realiza utilizando unas claves criptográficas. Además puede contar con la posibilidad de utilizar un "software" (Ibañez, 2018)[414] o de *Smart contracts*, en los cuales se puede desplegar órdenes predeterminadas y ser autoejecutadas dentro de la red.

¿Qué puede implicar el *"carácter distribuido"* jurídicamente hablando? El carácter comunitario de los componentes que pueden entablar relaciones entre sí en forma de consorcios, grupos de trabajo o asociaciones adquiriendo diferentes y múltiples formas jurídicas. También resulta de interés el papel que toma el incentivo económico vinculado a la propia introducción de los datos. Según IBAÑEZ, cualquier miembro de la red podría enviar datos para registrarlos si se cumplen las reglas de introducción o validación prefijadas, y cualquier nodo que esté autorizado al efecto puede recuperar datos. Todos los datos aparecen en todos los nodos simultáneamente, y además de forma necesariamente idéntica en todos los servidores o terminales conectados[415].

Para los profesionales juristas esta tecnología supone una auténtica revolución, sobre todo en el ámbito del comercio y de la industria, en las relaciones de las empresas con los particulares. En concreto, algunos de los retos más interesantes a destacar podrían ser los siguientes según IBAÑEZ (2018, 10):

i. "Los límites debidos de privacidad y confidencialidad de las transacciones y su régimen jurídico constitucional, administrativo y privado.
ii. Las relaciones jurídicas y económicas entre Administraciones y particulares.
iii. El concepto de mercado como espacio de transacción organizado y gobernado según estándares internos, y el modo de generar transparencia acerca de esos estándares, de forma democrática, participativa, cooperativa y entre iguales.

[413] ¿Qué es una DLT? Para este último autor, en primer lugar, se trataría de una tecnología de registros puesto que quienes operan lo hacen en el espacio de internet de una forma "registral" ya que quedaría constancia material pudiendo recuperar aquello que quedó grabado o registrado y, en segundo lugar, se podría tratar de un espacio donde las transacciones se guardarían y los sujetos podrían guardar con finalidades jurídicas como cotejar, archivar o custodiar. De esta manera quedarían constituidas las relaciones jurídicas con la eficacia que la Ley determine o las partes determinen adquiriendo una finalidad "probatoria".

[414] Vid. IBAÑEZ JIMENEZ, J. Wenceslao (2018). *Blockchain: Primeras cuestiones en el ordenamiento español.* Editorial DYKINSON

[415] Pero para introducir los datos es ineludible que se sigan las reglas de un protocolo o procedimiento de minado que consiste en palabras del autor "en la composición correcta de los pasos necesarios para obtener la encriptación de los datos que se persigue. Hay que tener en cuenta que esto exige de un esfuerzo de la capacidad computacional y por ende, del gasto eléctrico.

iv. Los conceptos mínimos de registro, registración, anotación de datos.

v. Las modalidades de participación de los agentes de contratación a distancia.

vi. La noción, constitución y administración de los sistemas de identidad digital de las personas físicas y jurídicas, merced a la combinación de la tecnología criptográfica con los mecanismos de distribución descentralizada de datos de identidad".[416]

¿Qué es una blockchain desde una perspectiva jurídica? En ocasiones se designa como *blockchain* a la propia DLT, de hecho, se llega a confundir ambos términos. El término anglosajón *"blockchain" -ad literam,* cadena de bloques- aunque se suele referir a la tecnología DLT, en verdad encajaría en una realidad más reducida, concretamente a los programas que forman el software que desarrolla esa tecnología DLT. Desde un punto de vista jurídico, las reglas del juego podrían ser (IBAÑEZ, 2018, 10):

a.) "El mecanismo de intercambio y los sistemas previstos para la cesión de datos que funcionan con los algoritmos establecidos y que resultan enlazados en la cadena de bloques

b.) El mecanismo para la creación de los bloques o secuencias independientes de los datos registrados

c.) Los sistemas técnicos y contractuales de relación entre los nodos desde los que se construye la secuencia o cadena temporal de bloques".

Ahora bien, resulta también, importante recordar la diferencia básica existente entre las diferentes redes de *blockchain*:

Redes públicas *(Bitcoin, Ethereum,)*	**Redes privada** *(Hyperledger o Ripple)*
El objetivo es "minar" la solución algorítmica que permite crear una *moneda* y obtenerla como *premio* de computación realizada.	El objetivo puede versar sobre cualquier contenido.

Deben ser conocidas en este trabajo (aunque sea pasando en puntillas sobre ellas) las aplicaciones más importantes de la tecnología *blockchain* como son las DAO (organizaciones autónomas descentralizadas) o las ICO (ofertas iniciales de moneda) y sus implicaciones legales El conocimiento de estos elementos y de otros resultará de

[416] *Vid.* Sullivan, C. , Burger, E. (2017) E-Residency and Blockchain. *Computer Law & Security Review* 460, 475. Recuperado de http://www.arifsari.net/isma500course/project/19.pdf . (Blockchain podrían facilitar nuevas formas de gestión de identidad al permitir a las personas "controlar el acceso a su información de identidad y crear, gestionar y utilizar una identidad de soberanía propia).

gran importancia para la correcta implantación de la tecnología teniendo en cuenta los aspectos legales, en particular, la protección de datos y privacidad de las personas.

Una DAO[417] es una "compañía" sin personalidad jurídica, autónoma y "descentralizada" no jerárquica, donde cualquier persona puede participar por acciones de la compañía, adquiridas a través de criptomonedas[418]. Éstas no cuentan con empleados, accionistas o mandos superiores ni tampoco tienen un objetivo empresarial específico, tampoco tienen costes altos puesto que no existen propiedades inmobiliarias o patentes. Se le puede considerar como una *organización basada en un código fuente autónomo, en la que cada función está programada en dichas instrucciones,* poniendo en marcha varios equipos al mismo tiempo a través de la *blockchain*. Tienen un carácter democratizador donde no existe un sistema burocrático, social, político o jurídico y donde sólo pueden modificarse sus directrices si el 51% de los miembros están de acuerdo[419]. Ahora bien, señalemos algunas de los *retos legales* que pueden plantear las DAO[420]. Posiblemente el mayor reto lo constituye la *ciberseguridad* y enfrentarse a posibles brechas de seguridad como las que ya han ocurrido con el *TheDAO*[421] en junio

[417] Ver más info: https://es.cointelegraph.com/news/dao-empresas-innovadoras-basadas-en-blockchain

[418] Una DAO es una colectividad que tiene como objetivo "la captación de fondos, bienes o derechos del público para gestionarlos e invertirlos en bienes, derechos, valores y otros instrumentos" (Art.1 de la Ley 35/2003 de 4 de noviembre de Instituciones de Inversión Colectiva). Según el fundador de *Ethereum*, *Vitalik Buterin*, la idea de diseñar una DAO era "codificar la declaración de la misión en un código; es decir, crear un contrato inviolable que genera ingresos, pague a la gente por realizar alguna función y encuentre por sí mismo el hardware donde ejecutarse sin necesidad de dirección humana". En una DAO el aspirante presenta una oferta, y los inversores de tokens votan a favor o en contra, exigiéndose el 20% de las mismas para que en caso de que salga adelante, se otorgaría un contrato para llevar a cabo el proyecto. El entorno facilita la innovación ya que el valor se basa en el propio valor de los proyectos y no en los cargos que poseen los interesados. a diferencia de las compañías convencionales, sino se entrega un proyecto a tiempo o no hay buen trato con el resto de colaboradores, los "accionistas" que votaron por dicho contrato retirarán sus *tokens*.

[419] Pongamos un ejemplo de DAO, en *e-Health,* que puede suponer la desaparición de intermediarios como los propios seguros de salud. el nuevo concepto de DAO, podría permitir un entorno seguro y de confianza con un registro inmutable y un seguimiento de auditoría sin que fuera necesario que nadie lo controlara en el sector asegurador con escenarios posibles de fraude (accidentes en el hogar o en el trabajo) en el reesembolso. Combinando el sistema P2P (peer to peer) y blockchain, se crearía un modelo de negocio de seguros autorregulado y autónomo para la gestión de pólizas y reclamaciones . Ver más info: https://www.pointnurse.com/blog/cyrus-maaghul-healthcare-blockchains-smart-contracts-and-daos/

[420] Como una DAO no tiene personalidad jurídica, la ley establece que su representación corresponde a una gestora, pero en una DAO la gestora y la propia DAO que capta fondos es una sola. Como hemos dicho, los participantes que aportan capital son aquellos que deciden a través de acuerdos. Tampoco estarían bajo la supervisión de la Comisión Nacional del Mercado de Valores ni de ningún otro organismo. Se podría llegar a parecer a una sociedad anónima (según la LSC), puesto que la aportación de fondos da como contravalor una serie de derechos (tokens), concretamente el del voto. El código del SC es la ley. Podría parecer que un DAO es un fondo de inversión cuyo consejo de administración lo forma el propio código del SC.

[421] *TheDAO* era una organización creada por un grupo de desarrolladores que desarrollaron un *smart contract* que desplegaron en la red para que cualquiera pudiera vincular Ethers (su moneda) a él, **algo que**

del 2016. Pero además, el otro reto es mantener la *privacidad* de los participantes. Como establece BUTERIN[422], "ni las empresas ni los individuos están particularmente interesados en publicar toda su información en una base de datos pública que pueda leerse arbitrariamente sin ninguna restricción por parte del propio gobierno, gobiernos extranjeros, familiares, compañeros de trabajo y competidores comerciales". Para este desarrollador "es mucho más difícil crear una tecnología de santo grial que permita a los usuarios hacer absolutamente todo lo que pueden hacer ahora mismo en una cadena de bloques, pero con privacidad; en cambio, en muchos casos los desarrolladores se verán obligados a lidiar con soluciones parciales, heurísticas y mecanismos diseñados para brindar privacidad a clases específicas de aplicaciones".

Por otro lado, una ICO *(Oferta inicial de moneda)* sirve para financiar el desarrollo de nuevos protocolos, algo parecido a una salida a bolsa al uso, pero con un protocolo descentralizado y sin un régimen regulatorio y legal definido (Preukschat y Molina, 157). Alguna de las ICO más conocidas están vinculadas al protocolo *Ethereum*, de hecho, ésta recaudó 15 millones de dólares hace más de 4 años. Esto l convirtió incluso en un competidor fuerte frente al protocolo *Bitcoin*, atrayendo a inversionistas. Una ICO puede denominarse también *token crowdsale* y tiene la consideración de una IPO (oferta inicial pública)[423]. ¿Dónde está una de las mayores dudas que pueden surgir en el sector jurídico-legal? Se encuentra en determinar si los *tokens* son valores pueden ser conceptualizados como valores. Si acudimos a la normativa aplicable en España, la Ley del Mercado de Valores, donde define los instrumentos financieros, nos encontramos con un concepto genérico de *valor negociable*, comprendiendo cualquier derecho de contenido patrimonial que por su

---

hicieron hasta 11.000 personas anónimas de todo el mundo. Estas personas aceptaron el código fuente abierto del programa como las normas a cumplir, sin que ninguno de ellos se diera cuenta de que había un error en él. Sin embargo hubo alguien que sí se dio cuenta de ese error, el cual permitía extraer Ethers sin el permiso de los demás. Resulta llamativa la carta que escribió donde declaraba reservarse acciones legales contra quienes actuasen contra él. Esta persona (anónima) fue explotando esta moneda y retirando cantidades crecientes de criptomonedas hasta hacerse con el equivalente a 50 millones de dólares. La pregunta es; ¿cómo podrían recuperar el dinero estos inversores? ¿a qué tribunal podrían acudir? ¿qué ley sería de aplicación? No parece haber respuestas claras al respecto por el momento. El mayor problema se encuentra en el anonimato ya que no se ha podido averiguar quien se llevó el dinero. Para más info: https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/

[422]Vid. https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/

[423] Las mayores v**entajas que genera una IPO son: (i) el a**cceso al capital**;** (ii) el cobro de beneficios por lo nuevos miembros en la venta de acciones; (iii) cuotas lucrativas para aseguradores o la CNMV; (iv) flipping es una manera rápida de obtener beneficios inmediatos en una OPI si el precio de mercado sube por encima del precio de suscripción.

configuración propia sea susceptible de tráfico generalizado e impersonal en un mercado financiero. No obstante, según *algunos autores*[424][425], ninguno de los instrumentos descritos en el listado que prevé dicha ley encaja con el objeto de una ICO, por lo que no estaríamos ni ante un "valor participativo" -por ejemplo, una acción- ni tampoco ante un instrumento del mercado monetario -por ejemplo, un pagaré- ya que no hay una representación de una deuda exigible a un emisor, ni tampoco a contratos financieros derivados relacionados con divisas, puesto que la Dirección General de tributos considera las criptomonedas como un medio de pago y no como dinero en sí mismo.

2. PARTICULARIEDADES JURÍDICAS GENERALES DE PROTECCIÓN DE DATOS EN BLOCKCHAIN Y DLT.

2.1.Los sistemas de gestión de identidad aplicables a blockchain

Ahora conviene centrarnos en algo muy relevante para el cumplimiento de la normativa y el RGPD: la identidad digital de las personas en el entorno tecnológico.

La identidad desde un punto de vista de análisis económico, es un bien de consumo y un activo de capital de la organización que enfatiza el rol transaccional de la identidad digital, con base en la posibilidad de mercadear con los datos de la identidad, con mayor o menor intervención y control del titular de dichos datos. El *Observatorio Europeo*

[424] Foz X., Martinero, J., Morales, JR, Carrascosa, C. (2017) *Blockchain: La revolución industrial de internet*. En *Aspectos legales de los ICO, Smart Contracts y DAO* (pp 176). Barcelona: Editorial Gestion2000.

[425] Los autores mencionados, mencionan a una corriente que opta por enmarcar a las ICO en la categoría de "crowdsourcing" y más concretamente, "el de donación o recompensa. Esta corriente se basaría en que se trataría de una donación por el trabajo realizado por los desarrolladores o bien ante una aportación a través de la cual lo que se obtendría sería un producto o un servicio asimilable a una licencia de software" Aunque sea una concepción viable, los autores citados creen que esta corriente tendrá difícil convencer al regulador del desinterés económico o actitud altruista de las personas que suscriben tokens. Tampoco como dicen, es que la normativa española de crowdfunding se pronuncie mucho ya que excluyen expresamente la propia captación de financiación a través de donaciones o de ventas de bienes y servicios y, por otro, las formas permitidas de captación de fondos bajo dicha normativa no son asimilables a esta figura. Los mismos autores señalan que parece que la reglamentación de las ICO pasa por su *autorregulación, de buenas prácticas* (Vid https://www.coincrispy.com/2018/11/27/codigo-de-conducta-para criptomonedas/?utm_medium=pushnotes) en la emisión y el establecimiento de procedimientos de gobierno corporativo que den confianza a los inversores. Así por ejemplo, en noviembre de 2018, se creó la Asociación de Mercados de Activos Digitales (ADAM) constituida por firmas financieras y tecnológicas cuyo objetivo es crear un código de conducta para la industria de criptomonedas donde se consiga aumentar la transparencia en la información verificada al público.

para Blockchain ha creado un informe[426] en diciembre de 2018 donde se sugirió la adopción por parte de los gobierno de un sistema de identidad basado en blockchain. Esas soluciones deberían ser controladas por el usuario para crear identidades seguras, privadas, únicas y comprobables que puedan ser verificadas sin revelar datos claves. En este mismo informe se reconoce la dificultad que han tenido las tecnologías centralizadas en conseguir esta meta. En la actualidad, nos encontramos pasando de la *"identidad en silos" a la "identidad autosoberana o descentralizada"*.

El SSI que utiliza la criptografía de conocimiento cero abre un mundo completamente nuevo de interacciones privadas poderosas[427] pero sobre todo lo que favorece es el cumplimiento del RGPD[428]. El sistema SSI permite crear un número indeterminado de identidades para diferentes usos. Por ejemplo, Rosa es titular de datos y además de utilizar el DNI para muchas cosas tendrá un credencial como sujeto fuente de un ensayo clínico, otro como usaria de una app de social diabetes, y otra como paciente de un consultorio médico local y otra como cliente de la aseguradora de salud Adeslas. Todos ellos son diferentes atributos de identidad, los cuales aumentarán con el paso del tiempo como es lógico (fuera del ámbito de salud también). Estas acreditaciones le podrán servir, respectivamente, para identificarse en un consorcio de blockchain como *HIT Foundation* y obtener token por permitir su acceso a la información médica registrada, para acreditar en una entrevista de trabajo donde le solicitan un certificado negativo de salud, para obtener descuentos en las pólizas de seguro de Adeslas gracias a su buen comportamiento de salud (1000 pasos por día), para

[427] Así por ejemplo, los sitios web y otros servicios pueden verificar que los usuarios son mayores de edad, sin necesidad de nombre, ubicación, edad o incluso cumpleaños; las compañías farmacéuticas pueden tener conexiones directas y privadas con pacientes que tienen recetas verificables para sus medicamentos, sin saber quién o dónde están esos pacientes; las personas pueden probar que son empleados de cierta compañía o ciudadanos elegibles para votar; que tienen un cierto puntaje de crédito; que su denuncia anónima o denuncia de irregularidades es creíble, etc., todo ello sin revelar sus nombres, direcciones u otros datos personales; al vender en forma privada un automóvil u otra propiedad, los propietarios pueden demostrar su propiedad legal sin revelar ningún dato personal; los usuarios de Internet pueden participar de forma seudónimo en los juegos, las redes sociales u otras comunidades en línea.

[428] Vid. https://medium.com/evernym/is-self-sovereign-identity-ssi-the-ultimate-gdpr-compliance-tool-9d8110752f89

obtener una cita en el hospital público o para recibir una notificación sobre el ensayo clínico del que es partícipe.

En todo caso, podrían tratarse de acreditaciones o credenciales que pueden ser comprobables mediante la firma digital registrada en blockchain desde el origen.

Desde Alastria[429], de hecho, se aboga por estos sistemas de identificación "atómicos", es decir, donde se utilizan identidades "una por una" y no "todas en una". Parece razonable pensar que entregar una fotocopia de DNI para acreditar la edad resulta excesivo; ¿es necesario comunicar el nombre de mis padres o mi dirección física o incluso mi número de ID? No sólo eso, sino que estaríamos arriesgando cumplir el principio de minimización que exige el RGPD. Por otro lado, mirando al futuro, nos encontramos con sistemas de identificación disruptivos -más allá de la clásica biometría de la huella digital o de las contraseñas- como la herramienta biométrica que usa las dimensiones cardíacas. En el Parlamento Europeo se está estudiando como regular posibles sistemas de identificación digital teniendo en cuenta el (problema) de la *interoperabilidad*[430] y la particularidad de que los datos personales biométricos de categoría especial sean salvaguardados por el RGPD.

Como decimos, SSI y blockchain permitirá empoderar al paciente y usuario de eHealth devolviendo el control de sus datos al mismo mediante la *tokenización de los atributos* de la identidad digital a través las *credenciales,* reclamaciones verificables o atestaciones a través de la web donde no existen terceros. En el *wallet* están contenidos los credenciales: quién o qué es el emisor del credencial y puede ser cualquier persona, organización o cosa a quién o qué fue emitido; si ha sido alterado desde que fue

---

[429] Pastor, Carlos de la Comisión de Identidad Digital del Consorcio Alastria (19 de Diciembre de 2018). En *Simposio Blockchain: Identidad Digital y el Reglamento General de Protección de Datos. Modelos prácticos y casos de uso.*

[430] Blockchain puede hacer un seguimiento de lo que ha cambiado en el registro de un paciente e incluso asignar una ID de paciente universal, pero no puede identificar al paciente correcto a menos que *todos los sistemas* que interactúen con esta base de datos central de la cadena de bloques puedan proporcionar la ID de paciente. Pero, además, se necesitaría almacenar tanto las identificaciones del paciente como las identificaciones de los *sistemas de registros de salud públicos*. Surgen dudas como; ¿para quién se establecería el bloque en primer lugar? El problema de interoperabilidad de HCE aún debe solucionarse, y ese problema no se resuelve mediante la asignación de pacientes o la cadena de bloques. Se requiere un compromiso universal por parte de los proveedores de EHR con el soporte de estándares como HL7 / FHIR, y también se requiere un compromiso universal por parte de los proveedores de HCE para abrir Apis.

emitido; si ha sido revocado por el emisor; y preferencias, opiniones, consentimiento legal y declaraciones.

5.2.1. El RGPD para SSI -Blockchain

A priori, cuando se oye la palabra blockchain tendemos a pensar en la incompatibilidad del RGPD. En palabras de PASTOR[431], "no solo es que no sea incompatible sino que Blockchain es la mejor opción para acreditar el borrado, salvo las excepciones legales contempladas".

Ahora bien, conviene señalar las siguientes cuestiones:

i. *Respecto a la base legitimadora del consentimiento*. El individuo introduce datos personales para obtener identidades digitales y el responsable del nodo debe estar en disposición de demostrar que la persona consintió en cederle los datos (Art. 7.1. RGPD).

ii. *Respeto al deber de información.* El participante *claimer*, pensemos en una startup de la industria farmacológica, que es responsable del tratamiento, deberá informar de ciertas cuestiones como la identidad y los datos del responsable, del DPO si lo hubiera, de los fines del tratamiento y la base legitimadora (ej. consentimiento o contrato o interés legítimo), los destinatarios o categorías especiales de datos personales (art 9 RGPD) como son los datos de salud o biométricos o genéticos, y en su caso, la intención del responsable de transferir datos internacionalmente.

iii. *Respecto a la finalidad del tratamiento de datos*. El individuo señala para qué fines quiere utilizar esa identificación. Por ejemplo, Rosa quiere identificarse como conductora (acreditando que tiene el carné de conducir) para alquilar un automóvil.

iv. *Respecto a la duración limitada del tratamiento.* El individuo puede determinar y dejar registrado en la cadena de bloques la duración del almacenamiento de ese testimonio. La API puede programar su eliminación automática en 2 años, por ejemplo.

v. *Respecto a la minimización.* Recordemos que el contenido que se guarda no es de la información personal sino el de los Hash del testimonio. Además, recordemos que el *smart contract* no se almacena en la cadena de bloques

vi. *Respecto a la seguridad del tratamiento y a las obligaciones de los responsables de tratamiento.* Los participantes o nodos validadores son responsables de implantar medidas de seguridad. Las políticas técnicas y de las reglas internas de responsabilidad[432] para un consorcio o red privada o semiprivada serán cruciales.

vii. *Respecto al derecho de supresión u olvido.* Como hemos dicho es posible puesto que la solicitud del borrado queda registrada (creando evidencia) en la cadena de bloques donde el nodo

[431] ***Supra cit.***
[432] Ver en https://alastria.io/assets/docs/responsabilidad.docx

responsable procederá a su solicitud y de no ser así, estaría incumpliendo la normativa salvo las excepciones establecidas.

5.2.1. El eIDAS para SSI -Blockchain

El *eIDAS*[433] (Reglamento europeo de identificación electrónica y los servicios de confianza para las transacciones electrónicas) se conoce como un habilitador para operaciones transfronterizas. Parte de la expedición, por los EEMM o bajo su responsabilidad , de medios públicos de identificación electrónica, o su reconocimiento, cuando sean privados. ALAMILLO[434] establece que "el Reglamento no regula los sistemas y medios de identificación electrónica, sino que debe ser el legislador quien lo haga, dentro de un espacio de discrecionalidad, incluyendo la posibilidad de que sea en régimen monopolístico (DNI-e), en modalidades de gestión directa (clave) o incluyendo la contratación del sector privado, incluyendo blockchain".

ALAMILLO, considera que el "*eIDAS* se hace extensible a Blockchain y posiblemente no sea necesario una regulación exclusiva para SSI. Esto favorecerá indudablemente que sea reconocida su aplicación a nivel transfronterizo". "Esta normativa no regula cómo hacer o proceder sino como un Estado Miembro puede notificar a otro Estado Miembro, lo que ha derivado a la creación de un metasistema y se ha definido un marco de trabajo global" (ALAMILLO). [435]"Esto tiene una serie de riesgos para la protección de datos como son los ataques al proveedor de identidad para conseguir robar las cuentas de los usuarios y la observación por parte del propio proveedor de identidad o por el nodo nacional la actuación de los sujetos empleando incluso metadatos o pruebas de conocimiento cero." Según el autor, "un modelo de identificación auto-soberana eliminaría estos riesgos, llegando a afirmar que incluso puede ser el único modelo legítimo".[436]

---

[433] Reglamento (UE) n ° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 , relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32014R0910

[434] **Alamillo, Ignacio.** ***Simposio Blockchain: Identidad Digital y el Reglamento General de Protección de Datos. Modelos prácticos y casos de uso.*** **19 de Diciembre de 2018.**

[435] *Ibídem.*

[436] Con este escenario y teniendo en cuenta su uso en el Mercado Único Digital, el autor considera conveniente la aprobación de un nuevo esquema de interoperabilidad de la identificación electrónica al amparo del Reglamento eIDAS. Algo que no exigiría ni su modificación ni ajustes. Lo que no cabe duda es que el papel de la autorregulación en SSI es imprescindible. Alastria, en este sentido, tiene posición de liderazgo indudablemente.

Respecto a las relaciones de ciudadanos con Administraciones Públicas, algo que nos interesa para el contexto de la sanidad pública y el cuidado de la salud, cabe señalar la disposición del art. 9.2. LPAC: "los interesados podrán identificarse electrónicamente ante las AAPP a través de *cualquier sistema* que cuente con un registro precio como usuario que permita *garantizar su identidad*". "Esta disposición deja vía libre para la utilización de la tecnología blockchain. No obstante, según el autor citado, " no se dice dónde se deben establecer las condiciones de dicho registro, ni establece requisitos mínimos para el sistema o los medios de identificación electrónico. No presupone que el sistema o el medio sea público, sino que deja espacio para la admisión de los del sector privado. Por lo que se admite el uso de sistemas." Por otro lado, llama la atención de lo establecido por el art. 9.3 LPAC y lo avalado en la STC 55/2018 a efectos de extender el reconocimiento de sistemas de identificación electrónica digital a todas las AAPP.

2.2.Los contratos inteligentes ("smart contracts")

2.2.1. Concepto y proceso de smart contract

Parece haber consenso[437] en el ámbito legal acerca de que no son tipos de contratos nuevos, sino nuevas formas de instrumentarlos para conseguir su ejecución automática, que no deja de ser la ejecución del previo acuerdo de voluntades convertido en código informático, sin mediar necesidad de confirmación previa y sin la posibilidad de alterar lo previamente pactado.

Por ejemplo, los "*Smart Contracts*" (o "contratos inteligentes", SC en adelante) permiten *automatizar bonificaciones* en áreas como los hábitos saludables, como por

[437] No obstante, *John Stark*[437] prefiere utilizar el concepto de "agente inteligente" o "*software agent"*. Este jurista describe las dos formas diferentes en que se entiende el término "contrato inteligente": 1.) Como *'código de contrato inteligente '*. Es enteramente operativo o transaccional. Esto implica la ejecución de agentes de software, normalmente como blockchain pero no necesariamente en un libro mayor compartido. La palabra 'contrato' en este sentido indica que estos agentes de software están ejecutando ciertas reglas u obligaciones y pueden tomar el control de ciertos activos dentro del libro mayor compartido. 2.) Como *'contratos legales inteligentes '* que se centra en cómo los contratos legales se pueden expresar y ejecutar en software. Esto, por lo tanto, abarca aspectos operativos, cuestiones relacionadas con la forma en que se redactan los contratos legales y cómo debe interpretarse la literatura legal. Hay varias ideas y proyectos que se centran en estos aspectos.

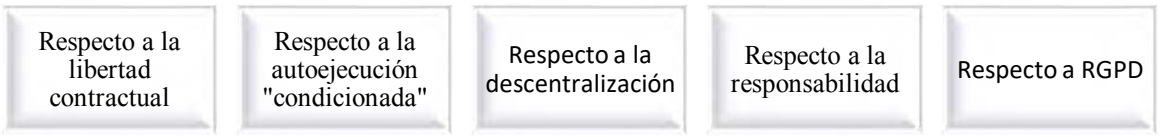
ejemplo, horas de ejercicio semanales o niveles de glucosa / colesterol entre limites, etc., Un ejemplo de esto es *Universal Health coin*[438] orientado a la prevención de la diabetes, obesidad y riesgo cardiaco, mediante la incentivación del paciente a seguir hábitos saludables ofreciéndole este incentivo en forma de una moneda virtual. Este modelo de blockchain estadounidense intenta dar soluciones sociales a sus sistemas de salud. En mi opinión, posiblemente, no sería aplicable para países europeos, pero nos sirve para detectar la función de los SC en estos sistemas tecnológicos.

Ahora bien, pongamos una utilidad más convencional: la gestión documental en el sector de la sanidad (atención médica). En estos casos, el usuario y en general todas las entidades poseen un certificado criptográfico que le identifica y cifra la información. La API facilitará a los participantes su utilización. El SC almacena la identificación y los permisos, pudiendo restringir quién tiene derecho a acceder a los datos del mismo. Posteriormente, cualquier otro usuario o entidad podría tener acceso a esa información si resulta autorizado por el sistema, pudiendo ser el proceso distribuido. La blockchain almacenaría metainformación sobre los documentos, y donde están guardados. La interfaz aunque debe estudiarse en cada caso las necesidades de cada actor y su forma de gestionar la información, en esencia, sería relacionar el trabajo de manejo de bases de datos documentales, que unido a los permisos cedidos y grabados en la blockchain permitiría a un usuario u otra entidad acceder a los mismos, siempre con una base criptográfica, y por tanto segura. En definitiva, una blockchain de salud podría funcionar como un gestor de control de accesos y permisos para datos y registros de salud.

2.2.2. Algunas cuestiones legales sobre SC

Partimos de la base que para considerar al SC como un "acuerdo legalmente vinculante y exigible ante los tribunales desde el punto de vista de la contratación", sería necesario que reuniese los requisitos legales de todo contrato, es decir; (i) que concurra el consentimiento de las partes; (ii) que tenga objeto lícito y (iii) una causa , es decir, un motivo válido, incluyendo la contraprestación. Ahora bien, dicho esto, convendría repasar las siguientes cuestiones para abordar un análisis jurídico completo.

[438] Ver *whitepaper* en https://uhx.io/wp-content/uploads/UHCWhitePaper-V2.3.pdf



i. *Respecto a la libertad contractual.* IBAÑEZ (2018,160) señala que "el legislador debe permitir que los operadores jurídicos en el momento de programar un SC, puedan diseñar clausulas parametrizables en los contratos que tienen lugar entre las partes para su ejecución en una blockchain dando cabida a la autonomía de la voluntad de forma que estas puedan flexibilizar las condiciones del negocio mediante opciones guiadas, bajo el principio de consentimiento informado, introduciendo avisos de mutuación si es preciso en el propio SC". También señala que "la regulación debería centrarse en incentivar eficazmente un comportamiento justo y jurídico de los operadores (emisores, inversores, mediadores y público en general) más allá de los intereses privados en el mercado"[439]. En todo caso, el contrato inteligente siempre hará exactamente lo que dice en su código, pero es probable que el contrato entre las partes incluya obligaciones más allá del propio código.

ii. Respecto a la *autoejecución condicionada*. Cuando sea difícil la interpretación del leguaje de programación, se podrán optar por soluciones mixtas que combinen previsiones en código con otras de *lenguaje natural.* Respecto a *la admisión de las condiciones*, algo lógico: no cabría sujetar una obligación a una condición que resulte imposible, contraria a las buenas costumbres o prohibida por la ley puesto que resultaría nula. Además, tampoco habría lugar para la autoejecución en el caso de condiciones complejas, subjetivas o requieran de interpretación externa. Se intuye que el código de los contratos inteligentes está sujeto a errores humanos. Hay que tener en cuenta que quien hace la oferta puede editar el SC para transacciones del futuro pero no puede revertir sus efectos para el SC existente. Ante vicios de consentimiento deberemos acudir a lo establecido en el código civil.

iii. Respecto a la *descentralización del SC.* Ante la inexistencia de autoridad central, ante cuestiones legales que pudieran surgir, convendría para demostrar que se ha realizado una transacción en una fecha concreta, conocer la identidad de los miembros. Los proveedores de servicios de identificación y certificación podrán acreditar la identidad y la integridad en el marco de la propia SC.

iv. Respecto a la *responsabilidad*. Si bien nadie es responsable de esta tecnología, si se pudiera identificar a alguien como causante de una agravio, se le podría exigir a éste responsabilidad civil o derecho de daños, y responsabilidad penal por posibles conductas de manipulación fraudulenta de la cadena de bloques según el art. 248.2 CP en relación con estafas mediante instrumentos informáticos, o en el art.

[439] AIBAÑEZ JIMENEZ, J. Wenceslao (2018). *Blockchain: Primeras cuestiones en el ordenamiento español.* Editorial DYKINSON

264 en relación con la alteración de documentos electrónicos ajenos (González-Meneses, 2017, 106)[440]".

v. Respecto algunas *cuestiones respecto el RGPD.* Antes de llegar a este apartado, hemos repetido en varias ocasiones que la información no se almacena en la cadena de bloques y que en todo caso lo que se almacena son los hash. También hemos afirmado que los SC deberán estar almacenados fuera de la cadena de bloques y, que para ello la API desarrollaría y programaría las cuestiones más importantes relacionadas con la protección de datos, como por ejemplo la eliminación automática de información personal registrada SC en 2 años. Ahora bien, al margen de las cuestiones que nos surgen respecto a la compatibilidad de la tecnología con la normativa, ponemos el foco en los propios smart contract y su compatibilidad con RGPD: *¿cuáles son sus posibilidades técnicas permiten realizar procedimientos de anonimización con las garantías debidas?; ¿cómo se repartirán las posibles responsabilidades por problemas de funcionamiento operativo de una SC por brechas de seguridad de la DApp?*

En todo caso, se aconseja es que desde el momento inicial del diseño de la plataforma y de programas participen expertos jurídicos de la tecnología en cuestión, y por supuesto, expertos en materia de protección de datos y blockchain.

2.3. Blockchain como herramienta de compliance.

Blockchain facilita el cumplimiento normativo a todo tipo de personas jurídicas, especialmente en organizaciones complejas o identidades que por su casuística y naturaleza requieren de herramientas que generen evidencias de cumplimiento normativo en materia de prevención de riesgos laborales[441] (*epis*[442] de trabajadores), de prevención de blanqueo de capital[443] o para el control laboral acceso[444] o en materia de PRL (epis)[445] o control de delitos y fraudes en entornos laborales con población infantil

[440] GONZÁLEZ-MENESES, Manuel (2017) ; *"Entender Blockchain: Una introducción a la Tecnología de Registro Distribuido"; pp 106.* Editorial Thomsosn Reuters Aranzadi

[441] Vid. http://prevenblog.com/blockchain-una-tecnologia-disruptiva-que-llega-para-cambiar-la-seguridad-y-salud-laboral/

[442] Vid. https://www.quironprevencion.com/blogs/es/prevenidos/importancia-epi-prevencion-riesgos-laborales

[443] Piénsese incluso que existen herramientas de blockchain para la prevención de blanqueo de capitales que contrastan bases de datos de clientes, empleados, proveedores y directivos con información de los lugares donde han estado, con quién se han reunido, en qué fechas, transacciones que han realizado, etcétera. Todo ello con bases de datos de personas condenadas, imputadas, países considerados paraísos fiscales que, con la ayuda de algoritmos permiten detectar actividades sospechosas y activar alertas. Pero se me ocurren más campos de aplicabilidad al margen del de frade y blanqueo de capitales.

[444] Vid. https://blog.ficharenltrabajo.com/

[445] Vid. https://beiota.com/. Se trata de una start up integradora con plataforma de datos propia.

laboral (diamantes de sangre[446]) o sistemas antiincendios. También puede posibilitar gracias a su característica de trazabilidad en sectores de minería, del medio ambiente[447], de la logística de medicamentos[448]. Las evidencias que generan no sólo sirven para "decorar" políticas de RSE o rellenar códigos de conducta sino como herramienta de responsabilidad proactiva.

Ahora bien , ¿por qué no extenderlo al *compliance en el ámbito de la protección de datos?* Varios son los motivos por los que podría ser ventajoso:

i. *La demostración del cumplimiento en la recogida del consentimiento expreso (Art. 7 RGPD) por parte del responsable del tratamiento.* El consentimiento permanece registrado en una red sin necesidad de almacenar los datos personalizados en la tecnología de la cadena de bloques. Del mismo modo, la retirada del consentimiento expreso podrá registrarse, encriptarse y sellarse el momento en el que se retiró.

ii. *La demostración del cumplimiento de la realización del análisis de riesgos y de la evaluación de impacto (Art. 25 RGPD)*. Las actuales herramientas tecnológicas en materia de protección de datos que hay en el mercado automatizan el análisis de riesgos y realizan evaluaciones de impacto de privacidad ahorrando gastos en servicios jurídicos o de consultoría. Pero blockchain, añadiría un "plus" al "petrificar" cualquier contenido de cualquier documento en el tiempo, o incluso, garantizar el comportamiento o la acción que ha ejercido una persona otorgando *transparencia. Blockchain* tiene un carácter descentralizador donde no necesita de una figura intermediaria pero se puede decir en sentido general que podría funcionar como un tercero de confianza.

iii. *Utilización de técnicas de encriptación* para otorgar mayor seguridad cumpliendo con la obligación del RGPD de la implementación de medidas técnicas y organizativas *(Art. 32 RGPD)*. De esta manera se demuestra, gracias a la naturaleza de esta tecnología y a la encriptación. Los hashes se almacenan en blockchain y los datos personales permanecen almacenados en una base de datos fuera de la red, los

[446] Vid. http://ec.europa.eu/trade/policy/in-focus/conflict-minerals-regulation/regulation-explained/index_es.htm También ver https://es.ihodl.com/analytics/2018-03-14/como-el-blockchain-ayudara-acabar-con-los-diamantes-de-sangre/

[447] Vid. https://www.pwc.com/gx/en/sustainability/assets/blockchain-for-a-better-planet.pdf

[448] FDA probará tecnología blockchain para el rastreo de suministro de medicinas. Vid https://www.coincrispy.com/2019/02/11/fda-probara-blockchain-medicinas/?utm_medium=pushnotes

nodos solo tendrán acceso a los hashes –números aleatorios sin significado para ellos–, cumpliendo así los principios de integridad y confidencialidad. la solución hash en blockchain consiste en la generación de hashes o identificadores únicos para los datos personales. Dicho hash quedaría almacenado en la red blockchain mientras que los datos personales, por su parte, se mantendrían en una base de datos externa, gestionada por el responsable de tratamiento que corresponda.

iv. *Empoderamiento al titular de derechos* y posibilitar la ejecución "automática" de la *clausula indemnizatoria económica (o no económica)?* ¿Por qué no combinar cloud y blockchain?[449] (Ver capitulo cloud computing e IoT).[450]

2.3.1. Casos reales de aplicación

Ejemplo 1. Alisys

El proceso iniciaría con el registro y la gestión del consentimiento: el usuario rellenaría el formulario para la recogida de datos personales que se contendrá en la base de datos personales (ej. IP, etc.), posteriormente se enviará la información generando un hash encriptado sin almacenar, y a continuación, se registrarán los datos de transacción y se desarrollará un SC. Por otro lado, el responsable del tratamiento puede consultar por medio un interfaz la existencia de ese registro.

Imagen. 45. Proceso de registro y gestión del consentimiento en Blockchain con Alisys. Fuente: Alisys

Ejemplo 2. Ebroker Blockchain NET. (Blockchain privada)

[449] Vid. https://guardtime.com/blog/blockcloud-re-inventing-cloud-with-blockchains

[450] Otra ventaja para negocio sería la propia *reducción de costes.* Para *IBAÑEZ*, "en el ámbito del cumplimiento de las reglas de protección de datos, específicamente, es palpable la reducción de costes, pues la automatización y simultaneidad del cumplimiento propias de Blockchain con Smart Contract y oráculos específicos, reducen los costes de cumplimiento relativas a las creación, manipulación, retención o conservación y destrucción de archivos informáticos, facilitando de modo sensible las labores internas corporativas relacionadas". *Vid.* IBAÑEZ JIMENEZ, J. Wenceslao (2018). *Blockchain: Primeras cuestiones en el ordenamiento español.* Editorial DYKINSON. Pp 174.

Es un proyecto de innovación formado por más de 600 nodos constituida por corredores de seguros para interoperar e intercambiar información con las entidades aseguradoras en el marco de otras redes privadas o semipúblicas como el *Consorcio Alastria* y gestionar cuestiones como el cumplimiento normativo en protección de datos.

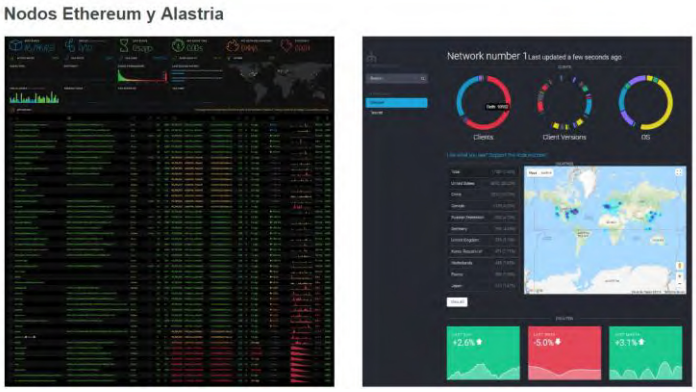


Imagen. 46. Nodos Ethereum y Alastria. Fuente: Alisys

Ejemplo 3. Blocknitive - Asentify (Blockchain Privada)

Quizás es una de las soluciones más comprometidas con el RGPD para empresas de perfil de publicidad y marketing. Pretender resolver el problema de almacenar la base de datos y control de la legitimación

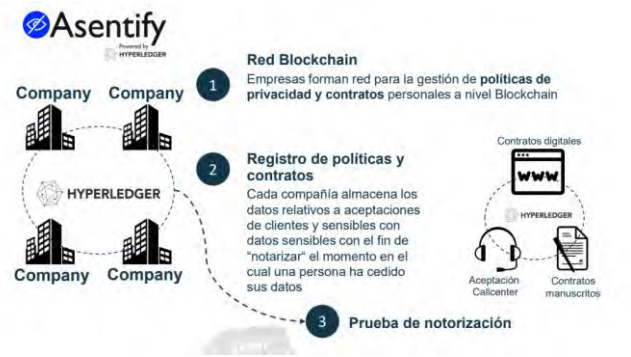


Imagen. 47. Red blockchain y registro de políticas y contratos. Fuente: Asentify

Los usuarios de las empresas que estén incluidas quedarán registrados en Blockchain de Hyperledger Fabric permite que las compañías *almacenen los datos relativos al otorgamiento del consentimiento* expreso -como base legitimadora del tratamiento- con el fin de "notarizar" el momento, URL, dispositivo y otra información relativa en el cual una persona ha aceptado dicho tratamiento. Al tratarse también de una blockchain privada provee mayor garantía de privacidad añadiendo una capa de permiso para personalizar el papel de cada participante en la red. Solo las empresas propietarias de esta información, son las únicas que pueden acceder a sus datos

3. PARTICULARIEDADES JURÍDICAS ESPECÍFICAS DE PROTECCIÓN DE DATOS EN BLOCKCHAIN Y DLT.

Ya el SEPD[451] llamó la atención a los expertos en privacidad en el informe anual del 2016 para examinaran los conceptos de la tecnología blockchain y la forma mejor de implementar el RGPD.

3.1.El tratamiento de datos personales y el consentimiento en blockchain.

En el caso de esta tecnología podría referirse a cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjunto de datos personales, por ejemplo, por "*procedimientos automatizados"* como el *"registro"* o la *"difusión"* o *"cotejo"* o *"cualquier forma de interconexión"* (art. 4.2 RGPD). Por ejemplo, una consulta de datos de salud es una petición de acceso a datos clínicos de un consumidor a la red. La respuesta puede provenir de múltiples proveedores, ya que los datos de un paciente pueden estar fragmentados en múltiples centros médicos o hospitales. Las consultas pueden ser sobre un paciente concreto o agregadas sobre datos anonimizados. Toda acción en la red (tanto consultas, como permisos de acceso, etc.) queda registrada en la blockchain, constituyendo un log de accesos inmutable y facilitando por tanto las auditorías. Como estos accesos se registran en tiempo real, sería incluso posible el desarrollo de un sistema de alarmas para detectar accesos inusuales a datos (EDPS,2016)[452] .

El tratamiento de datos se puede producir por la intervención de los usuarios, nodos validadores y mineros cuando envían, verifican y almacenan o registran las transacciones. Tengamos en cuenta dos tipos puntos de vista respecto al tratamiento en Blockchain:

i. En primer lugar, pensemos en *el tratamiento de datos como servicio (per se),* por ejemplo, el sistema de dinero electrónico entre igual e igual. Los medios serán el software y el hardware que los nodos y mineros utilizan para este fin. Estos últimos son quienes deciden sus propios fines, el hardware y el software a utilizar. Dicho esto, entenderíamos que los *nodos validadores y mineros* serán los *responsables del tratamiento.*

[451] EDPS. (2016). *Annual Report.* Recuperado de https://edps.europa.eu/sites/edp/files/publication/17-04-27_annual_report_2016_en_1.pdf

[452] *Revista de la Sociedad Española de Informática y Salud*. Número 128. Abril 2018. Blockchain en Salud. ¿Quimera o realidad?. Recuperado de https://seis.es/wp-content/uploads/2018/04/128.pdf

ii. En segundo lugar, pensemos en el tratamiento de datos que se produce en una *transacción individual y específica,* del que nos referiremos a partir de ahora. Los medios en este caso son elegidos por la propia plataforma *blockchain*. Los usuarios proporcionan los datos personales en el sistema al enviar sus transacciones. El papel de los nodos y los mineros es facilitar el acceso a la base de datos y el papel de los usuarios determinar qué datos se almacenan. Dicho lo cual, entenderíamos que los *responsables del tratamiento* serían los *usuarios* (o participantes).

Este ejemplo de caso de uso comienza con un médico que agrega un nuevo registro siguiendo los siguientes pasos:

i. La información del registro se almacena en el sistema de base de datos existente del proveedor.
ii. Se publica una referencia hash a los datos (con los permisos de visualización apropiados) en la cadena de bloques a través de nuestro cliente Ethereum y la biblioteca de API de backend.
iii. El paciente puede recuperar y descargar estos datos de la base de datos del proveedor, luego de que el controlador de acceso a la base de datos verifique el *blockchain* para confirmar sus derechos de acceso y propiedad.

Por otro lado, el *consentimiento* (art. 4.11, 6.1.a y 7 RGPD) *expreso* que es obligatorio en la RGPD no entraría en conflicto, sino todo lo contrario, podría resultar un elemento clave para el cumplimiento puesto que el usuario verifica y valida los datos antes de que se agreguen a la cadena de bloques. La prueba de este consentimiento bien puede ser informado, sin embargo, debido al anonimato y el uso de seudónimos, es poco probable que los interesados den el consentimiento para el tratamiento. El problema de la asunción errónea de legitimación en entornos de ensayos clínicos ha hecho que investigadores[453] estudien el potencial de blockchain como solución. Y es que la FDA estadounidense ha informado que casi en el 10% de los ensayos no se obtuvo un consentimiento informado por escrito o los formularios de los individuos estaban sin aprobar o los documentos otorgaban un consentimiento no válido.

3.2.El concepto de "dato personal" en blockchain.

Partimos de la base de que un dato de salud o médico o clínico es cualquier pieza de información clínica referente a un paciente. Puede tener cualquier granularidad,

[453] **Vid. Benchouf M.;Ravaud P., (2017) Tecnología blockchain para mejorar la calidad de la investigación clínica. *BMC*. Recuperado de https://trialsjournal.biomedcentral.com/articles/10.1186/s13063-017-2035-z#CR36**

tamaño y formato, ya que no se almacenará en la blockchain. Según el art. 4.1. RGPD, *dato personal* es:

> "Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse**,** *directa o indirectamente*[454], en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona."

También, sería importante, llegados a esta altura, analizar la concepción de la dirección IP como dato personal por los tribunales nacionales y supranacionales. EL TS en su sentencia de 3 de octubre de 2014[455] (FJ 4) establece, sin dejar lugar a dudas, que la IP debe ser considerada como dato personal señala concretamente:

> *"las direcciones IP son datos personales, en el sentido del artículo 3 LOPD, ya que contienen información concerniente a personas físicas "identificadas o identificables" y añade que*

---

[454] Pero, ¿a qué se refiere el GT29 con los términos *"directa" o "indirectamente" identificable*? Respecto a la expresión "directamente", el GT29 (Ver Opinion 4/2007 on the concept of personal data. Ver en https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf) analizó hace más de una década estas expresiones afirmando que la identificación se logra normalmente a través de piezas particulares de información que nosotros pueden llamar "identificadores" y tienen una relación particularmente privilegiada y cercana con el individuo particular. Ejemplos son signos externos de la aparición de esta persona, como altura, color de cabello, ropa, etc. o una cualidad de la persona que no puede ser percibido inmediatamente, como una profesión, una función, un nombre, etc. Pero también una persona puede ser identificada por su número de teléfono, la matrícula del automóvil, el número de la seguridad social o por una combinación de criterios significativos que le permita ser reconocido al reducir el grupo al que pertenece (edad, ocupación, lugar de residencia, etc.). Por ejemplo, un apellido muy común no sería suficiente. La noción de persona identificada implica más a menudo una referencia al nombre de la persona, pero a veces el nombre tiene que ser combinado con otras piezas de información como son la fecha de nacimiento, los nombres de los padres o una fotografía de cara para evitar confusiones entre esa persona y otros. Pero, además, también se puede identificar a una persona por una serie de diferentes relaciones legales y sociales como registros médicos, cuentas bancarias y registros de educación.
Y respecto a la expresión "indirectamente" hemos de tener en cuenta que si los datos están destinados a ser almacenados durante un mes, no se puede anticipar que la identificación sea posible durante el "vida útil" de la información, y no deben considerarse datos personales. Sin embargo, si se pretende que se mantengan durante 10 años, el responsable debe considerar la posibilidad de identificar y lo que puede hacer que los datos personales en ese momento. Por ejemplo, la publicación en una revista científica de placas de rayos X junto con el primer nombre de la paciente combinando el conocimiento por parte de sus familiares o conocidos de que ella sufrió una cierta dolencia convirtió en que la paciente fuera identificable para un número de personas y se consideró a la placa de rayos X como dato personal. Otro ejemplo, hospitales y médicos transfieren datos a una empresa de investigación farmacéutica datos de registros médicos de sus pacientes sin utilizar nombres de pacientes. Sólo se asignan números de serie al azar a cada caso clínico. Los nombres de los pacientes permanecen exclusivamente en posesión de los respectivos médicos obligados al secreto profesional. Y estos datos no contienen información adicional que permita su identificación con posibles combinaciones como en el ejemplo anterior.

[455] Sentencia del Tribunal Supremo, Sala de lo C.A. 3896/2014, de 3 de Octubre de 2014, Rec 6153/2011. Recuperado de http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=7195354&links=&optimize=20141023&publicinterface=true

"…no cabe duda que, a partir de la dirección IP puede identificarse directa o indirectamente la identidad del interesado".

En consecuencia, señala que si se desea tratar este dato, debe cumplirse con los deberes de consentimiento e información previstos en la normativa de protección de datos; pues, el hecho de que un usuario "*conozca que su dirección IP es visible y puede ser conocida, no significa que acepte, de forma inequívoca, su uso y tratamiento por terceros, ni que consienta de forma específica el tratamiento de sus datos".*

Por su parte, el TJUE en la Sentencia[456] de 19 de octubre de 2016 (*Patrick Beyer v. Bunderespublik Deutschland*) determina que:

"una dirección IP dinámica registrada por un proveedor de servicios de medios en línea con ocasión de la consulta por una persona de un sitio de Internet que ese proveedor hace accesible al público constituye respecto a dicho proveedor un dato personal, en el sentido de la citada disposición, cuando éste disponga de medios legales que le permitan identificar a la persona interesada gracias a la información adicional de que dispone el proveedor de acceso a Internet de dicha persona".

Pero, además, si concebimos al dato personal incluido en un fichero, deberíamos acudir al RPGD y la ex LOPD para aclarar posibles dudas. Según el art. 4.6 RGPD:

"Fichero es todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado o *repartido de forma funcional* o geográfica".

En este sentido y teniendo en cuenta la naturaleza de la DLT, podemos pensar que los datos personales se almacenan o registran de forma repartida en la cadena de bloques (o incluso, fuera en modo *off-chain o sidechain*). Según el art. 3.b de la ex LOPD:

"Fichero es todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o *modalidad* de su creación, *almacenamiento,* organización y acceso".

Teniendo en cuenta ambas definiciones entendemos que son ficheros también las copias automáticas registradas en todos los nodos teniendo en cuenta su forma particular de estar almacenado y repartido y la modalidad de almacenamiento. Por otro lado, es de destacar el considerando 26 RGPD, donde el legislador señala que los datos personales *pseudonimizados* se deben considerar información sobre una persona física

[456] Sentencia del TJUE, Sala 2ª. Asunto C-582/14, de 19 de octubre de 2016. Recuperado de http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=1314731

identificable. Además, señala que para determinar si una persona física es identificable, debe tenerse en cuenta *todos los medios* que *razonablemente* pueda utilizar el responsable del tratamiento o cualquier otra persona *para identificar al individuo*. Por ejemplo, "las claves y direcciones públicas desechables de Bitcoin pueden calificarse como datos personales" (*FINCK,* 2018, 12)[457].

De hecho, el propio TJUE[458] estableció que se puede consideran como "datos personales" incluso cuando sólo un tercero tiene los datos adicionales para identificar a la persona. En este sentido, se señala;

> "...se debe determinar si la posibilidad de combinar una dirección IP dinámica con los datos adicionales del proveedor de servicios de Internet constituye un medio razonablemente para que puedan ser utilizados para identificar al titular de los datos".

No obstante, como ya comentaremos, no resulta fácil igualar un proveedor de servicios de Internet como responsable del tratamiento a un proveedor de *blockchain* por la sencilla razón de que no existe tal figura como tal. En todo caso, hay que tener en cuenta que puede ser posible determinar, por ejemplo, las identidades de usuarios de *Bitcoin*[459] -en *blockchain* públicas- combinando registros de intermediarios con la cadena de bloques y con la dirección de bitcoin o combinando la clave pública con direcciones IP. Por eso, en ocasiones se pueden considerar a las direcciones bitcoin y a las claves públicas como datos personales. Hay algo que es de especial interés y tiene que ver con la posibilidad de que algunos datos personales se almacenen fuera de la cadena de bloques de forma encriptada en otra base de datos (en modo de *off-chain o sidechain*) como mencionaremos más adelante.

---

[457] Finck, Michèle, Blockchains and Data Protection in the European Union (November 30, 2017). Max Planck Institute for Innovation & Competition Research Paper No. 18-01. Available at SSRN: https://ssrn.com/abstract=3080322 or http://dx.doi.org/10.2139/ssrn.3080322

[458] Sentencia Breyer v. Alemania, C-582/14, § 31, 39 (ECJ 2016)- Recuperado de http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN

[459] Por ejemplo, en la página de *Bitcoin.org* se puede encontrar la siguiente información: "todas las transacciones de Bitcoin son públicas, rastreables y almacenadas permanentemente en la red de Bitcoin. Las direcciones de bitcoins son la única información utilizada para definir dónde se asignan los bitcoins y dónde se envían. Estas direcciones son creadas privadamente por las carteras de cada usuario. Sin embargo, una vez que se usan las direcciones, se ven afectadas por el historial de todas las transacciones en las que están involucrados. Cualquiera puede ver el saldo y todas las transacciones de cualquier dirección. Como los usuarios generalmente tienen que revelar su identidad para recibir servicios o bienes, las direcciones de Bitcoin no pueden permanecer completamente anónimas. Como la cadena de bloques es permanente, es importante tener en cuenta que algo que no se puede rastrear actualmente puede volverse trivial para rastrear en el futuro". Las recomendaciones que mantienen son: utilizar nuevas direcciones para recibir pagos, tener cuidado con los espacios públicos, tener en cuenta que la dirección IP puede ser registrada (Tor), limitar los servicios de mezcla.

3.3.Tipos de datos en Blockchain y DLT.

Por tanto, si bien no todos los proyectos de *Blockchain* implican el procesamiento de datos personales, en la práctica, muchos usos de esta tecnología requieren la manipulación de estos datos, tanto en términos de contenido como de información de los participantes. Antes de continuar y analizar qué datos personales pueden existir, pensemos en ejemplos de datos -generales- en DLT y *blockchain* como los siguientes:

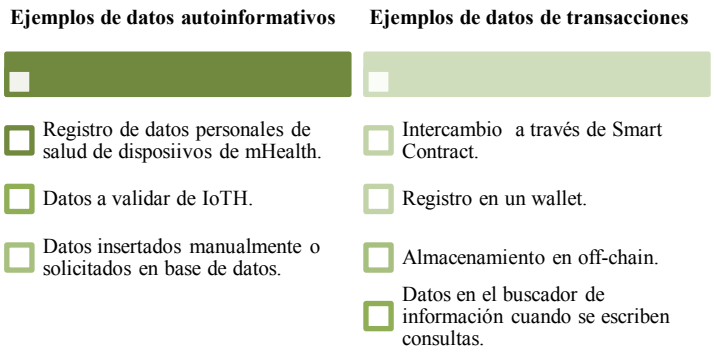


Imagen. 48. Ejemplos de datos en DLT y Blockchain. Fuente: Propia..

En esta línea, podríamos distinguir *dos tipos de datos personales*:

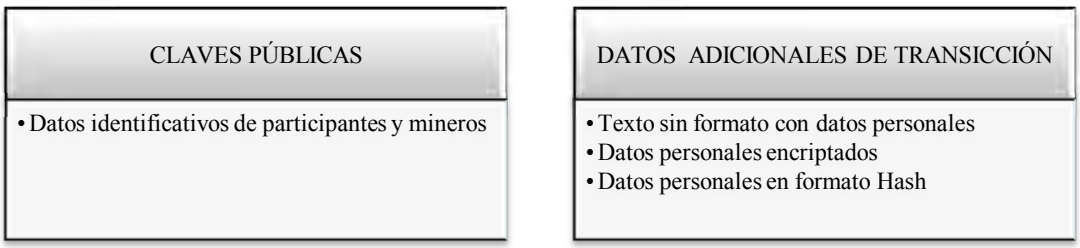


Imagen. 49. Tipos de datos personales en DLT y Blockchain.Fuente: Propia.

i. Claves públicas: *los datos identificativos de participantes y mineros.*

La CNIL[460], la autoridad de control francesa de protección de datos personales considera a los *datos identificativos* de mineros y participantes como un tipo de categoría de *dato* (pensemos en participantes como pacientes / consumidores / médicos /

[460] CNIL (2018) *Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data*. Recuperado de https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data

hospitales/ investigadores/ empresas farmacéuticas / sector público / comunidad científica). Cada participante tendrá una clave pública que garantizará la identificación del emisor y el destinatario de una transacción. Las claves públicas son una serie de letras y números que permiten la identificación seudónima de una persona física o jurídica con fines transaccionales o de comunicación. Esta autoridad considera que no es posible minimizarlos (Art. 5.1.c RGPD) más y que su vida útil está, en esencia, alineada con la vida útil de la propia Blockchain.

Ahora bien, *¿las claves públicas son realmente datos anónimos?* Según la CNIL, "una clave pública es información que 'ya no puede atribuirse a un sujeto de datos específico' a menos que se corresponda con 'información adicional', como un nombre o una dirección. Cuando estos dos conjuntos de información *se combinan*, la identificación es plausible, explicando por qué las claves públicas no pueden calificar como datos anónimos. Para que los datos se califiquen como identificación anónima se deben evitar dicha identificación de manera irreversible. El breve historial de los DLT demuestra que, a pesar de la identificación con cifrado asimétrico, sigue siendo posible". Pensemos en lo que dice la Agencia respecto a que se pueden identificar a los usuarios ya que ellos voluntariamente otorgan información, por ejemplo, revelando la clave pública para recibir los fondos. Como decíamos en párrafos anteriores, las claves públicas se pueden rastrear hasta las direcciones de IP (información que se registra en las transacciones que se realizan) y en consecuencia, se puede conseguir identificar al usuario. Los datos personales sometidos a una pseudonimización son datos personales, de igual modo.

ii. Los *datos adicionales de las transacciones*.

Si los usuarios de la plataforma son personas físicas, las direcciones de correo electrónico del remitente y del destinatario serán datos personales. Puede resultar más obvio aún si se esas direcciones identifican a personas. Pensemos, por ejemplo, en los certificados médicos o registros de un wearable o un HCE con datos personales de salud que hacen identificables a las personas, se transfieren de un sujeto a entidades públicas o privadas. En este sentido, hay que tener en cuenta que aunque el proveedor de la plataforma los convierta en pseudonimizados no dejan de ser datos personales (considerando 26).

Según *FINCK*, estos datos se pueden almacenar en una cadena de bloques *-in-chain-* de tres maneras alternativas: *en texto sin formato, en forma encriptada o mediante hash en la cadena.* Según la autora:

> "en primer lugar, los datos personales almacenados en una cadena de bloques en texto sin formato permanecen claramente como datos personales para el RGPD, por lo que esta opción no merece ningún otro análisis. En segundo lugar, cuando los datos están encriptados, se puede acceder a ellos con las claves correctas, lo que significa que no se anonimiza irreversiblemente. Los datos cifrados se pueden conectar, por ejemplo, al sujeto de los datos cuando las transacciones se efectúan para productos fuera de la cadena o cuando los cryptoassets se convierten en moneda fiduciaria. El cifrado se considera una técnica de pseudonimización en el régimen de protección de datos de la UE, dado que el sujeto de los datos todavía puede identificarse indirectamente por lo que no se puede considerar como una técnica de anonimización. La conclusión de que los datos transaccionales que se han cifrado siguen siendo datos personales para los fines del RGPD es, por lo tanto, inevitable. En tercer lugar, los datos transaccionales que han sido sujetos a un proceso de hashing también son datos personales según el RGPD. El GT29 ha sido inequívoco en cuanto a que el hashing constituye una técnica de pseudonimización, no de anonimización, ya que todavía es posible vincular el conjunto de datos con el sujeto de los datos".

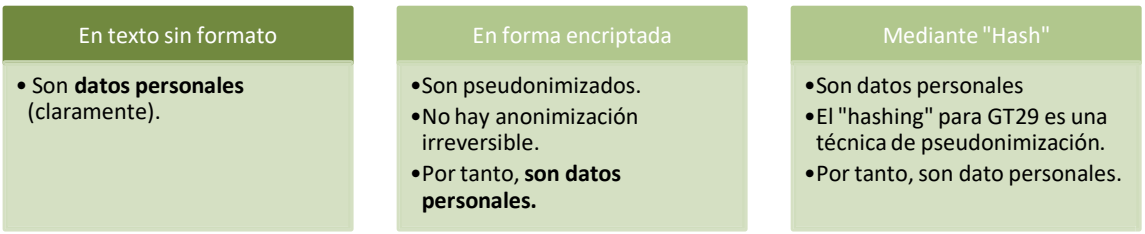


Image 50. Tipos de datos personales de transacción adicionales en DLT y Blockchain. Fuente: Propia.

Respecto a la tercera forma de dato personal, he de señalar que la AEPD[461] se ha pronunciado en este sentido afirmando en su Guía de orientaciones y garantías en los procesos de procedimiento de anonimización de datos personales (2016):

> "…Sin embargo, un algoritmo de hash por sí solo no es suficiente para hacer irreversible la anonimización, ya que pequeñas cadenas de texto como, por ejemplo, los microdatos correspondientes al código postal de una persona, un número de teléfono, etc., pueden ser fácilmente reidentificables con un programa informático que genere cifras consecutivas y sus correspondientes huellas digitales".

[461] Para más info: https://datos.gob.es/sites/default/files/doc/file/orientaciones_y_garantias_anonimizacion_0.pdf Pág. 14.

Así por ejemplo, en *HIT Foundation* existen diferentes tipos de registros de datos, y en todo caso, estructurados y digitalizados:

a. Datos de autoinformativo puro.
b. Datos a validar por profesionales de la salud. Por ejemplo, datos de apps (mHealth) o dispositivos IoTH conectados a monitores de glucosa en sangre.
c. Datos ingresados manualmente (por cuestionario) o datos escaneados (captura de datos).
d. Datos pedidos a través de bases de datos existentes.

La inserción de los datos requiere aplicar el mecanismo de *doble clave criptográfica asimétrica*. Las dos claves pertenecen a la misma persona que recibirá el mensaje. Una clave es *pública* y se puede entregar a cualquier persona, la otra clave es *privada* y el propietario debe guardarla de modo que nadie tenga acceso a ella. A continuación, exponemos un ejemplo de cifrado asimétrico de mensaje:

Image 51. Ejemplo de proceso de cifrado asimétrico de mensaje.

1. Ana /emisores redacta un mensaje o envía pdf o archivo de datos
2. Ana /emisores manda el mensaje cifrado con la clave pública del destinatario
3. Ana/emisores envía el mensaje cifrado al destinatario
4. Los destinatarios reciben el mensaje cifrado y lo descifran con su clave privada
5. Los destinatarios ya pueden leer el mensaje original que mandaron Ana

Este cifrado se aplicarán, también, a las *blockchain distribuidas y centralizadas* de la que nos centraremos más adelante. Estas podrán ser de uso *privado* por *una persona jurídica –pacientes o usuarios de eHealth- o empresa -startup* tecnológica o compañía farmacéutica- o grupos de empresas -asociaciones empresariales- o por una corporación de derecho público -la propia Administración- donde se comparten los datos a través de los nodos.

¿Cómo funcionan técnicamente las hash de la blockchain? Recordemos que aquello que identifica cada bloque de cadena es sobre todo sus identificadores únicos –

hashes-, que son secuencias alfanuméricas (ej. 0000057ec2fda71) que funcionan a través de la creación de transiciones (por ejemplo, pensemos en el traspaso de HCE o datos personales de salud de dispositivo *wearable m-health* o en la venta de los mismos para investigación a compañías farmacéuticas).

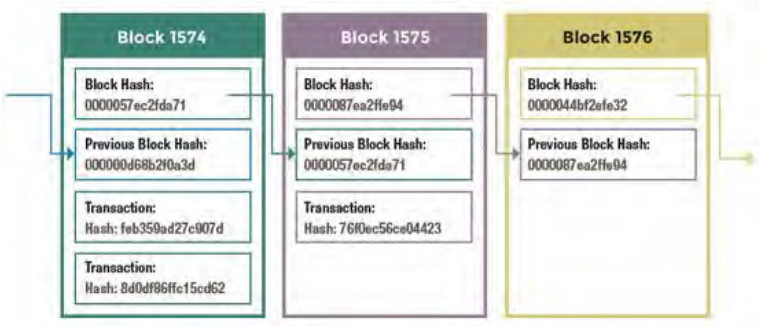


Imagen 52. Ejemplos de Block hash. Fuente: AddVANTE

Cada vez que se aplica una función algorítmica a los datos que se van a registrar en la cadena, aparece el *"hash"*. Cada bloque de datos se vinculará a un hash identificador determinado y único, cuyas funciones principales serían, identificar y conectar o ligar bloques haciendo irrompible esa cadena. Por ejemplo, este es un ejemplo de bloque con hash y datos personales (nombre y apellidos, edad) encriptados:

Bloque 3313
Hash: d41d8cd98f00b204e9800998ecf8427e (32)
Prev_hash: b026324c6904b2a9cb4b88d6d61c81d1 (32)
Data: "{ "name":"John", "age":30, "car":null }" (1024)

Image 53. Ejemplo bloque hash. Fuente: Medium.com

Esta cadena de bloques identificadores con sus claves facilita el seguimiento o trazabilidad de todos los datos. Introducir cualquier cambio de datos supondría una alteración de todos los hashes, y en consecuencia, los siguientes valores no se podrían registrar[462]. Sobre esta cuestión trataremos más adelante en relación a la compatibilidad de la naturaleza de esta tecnología y la regulación en materia de protección de datos o RGPD. Por tanto, sólo los bloques se podrán encadenar[463] y unirse a los anteriores

[462] La imposibilidad de introducir una variación de datos y esto se traduce en el efecto altamente disuasorio del fraude (*IBAÑEZ,* 2018,13) ya que no podrá retroceder en la cadena en caso de que quisiera eliminar un registro -aunque fuera un solo bit- ya que no permitiría la cadena, rompiéndose en cascada. Esta alteración aunque es posible -técnicamente hablando- los nodos se podrían oponer a ejecutarse salvo por el concurso de la mayoría de los nodos. En todo caso, esa posible alteración se podría producir con el llamado *"protocolo de consenso"* derivado de la voluntad de los nodos. Es decir, cada protocolo conlleva la existencia de un pacto entre los nodos (expreso o tácito) pero jurídicamente válido.

[463] Cada sistema de "encadenamiento de datos" al margen de la información encriptada contiene (*IBAÑEZ*, 2018, 14) : i. El *sello de tiempo* (fecha y hora del bloque y sus transacciones) que usando el mecanismo conocido la cual probará la fecha en los sistemas de firma avanzada y probará la fecha de encadenamiento y registro de la cadena de bloques; ii. los *hashes alfanuméricos*, hexadecimales, únicos; iii. un *nonce o número oculto* el cual forma un problema matemático que resuelto permite a los mineros o validadores cerrar el bloque y engarzarlo a la cadena; iv. los *datos o información encriptada*.

si se realiza de forma consentida siguiendo los protocolos de consenso que permiten identificar y verificar mediante una prueba matemática[464] [465].

3.4.Los sujetos jurídicos en el tratamiento en blockchain.

Previamente a profundizar sobre la posición jurídica de los actores o participantes de esta tecnología, hagamos un repaso de cómo quedaría un posible escenario de blockchain permisionada de eHealth para proceder a "desmenuzar" los entresijos de los miembros y sus implicaciones jurídicas. Partiremos de un escenario tomando a Blockchain como un sistema de intercambio de información[466] [467].Aunque será imprescindible determinar los roles y usuario, así como la información que debería registrase *onchain* y cuál debería figurar *offchain*, teniendo en cuenta para ello cuestiones como la capacidad de procesamiento y la naturaleza del dato.

[464] Hay un hecho que llama la atención, y es que en caso de problemas entre nodos se puede llegar a producir bifurcaciones o *"forks"* o eslabones divergentes donde el *blockchain* se separa temporal o definitivamente. No obstante, se pueden consolidar si algunos nodos siguen el código fuente de un nuevo proyecto. Suele ser extraño, pero ocurre en redes *blockchain* públicas. Los mineros u operadores habrán de determinar qué solución criptográfica tiene el problema algorítmico que permite cerrar cada eslabón de forma definitiva. Quizás en unas décadas, se podrá cambiar lo registrado una vez que evolucione la computación cuántica. González-Meneses (2017, 107) señala que en materia de seguridad de blockchain todo es muy relativo, y la desintermediación tiene también su coste. Este mismo autor ya estableció que la propia técnica criptográfica no es incuestionable y además, señaló su preocupación por la vulnerabilidad de la tecnología en el contexto de la computación cuántica que se caracteriza por un incremento exponencial de la potencia de cálculo respecto de la informática tradicional.

[465] Al decir de expertos en criptografía, como Javier DOMINGUEZ GÓMEZ (Seminario Blockchain: aplicaciones en el sector eléctrico. ICAI -Observatorio Blockchain Everis Comillas, 24.10.2018) en AIBAÑEZ JIMENEZ, J. Wenceslao (2018). *Blockchain: Primeras cuestiones en el ordenamiento español.* Editorial DYKINSON

[466] *Supra Cit.*

[467] Según Carretero et. al. (2018), el logro de la tecnología Blockchain no es un problema tecnológico, ya que existe la tecnología que permite compartir toda esta información de una manera abierta, plástica e inteligente (véase *LinkedData*). Más bien, "el reto es *superar un problema de confianza*, confianza en la pertenencia de los datos, y en la responsabilidad de su consumo".

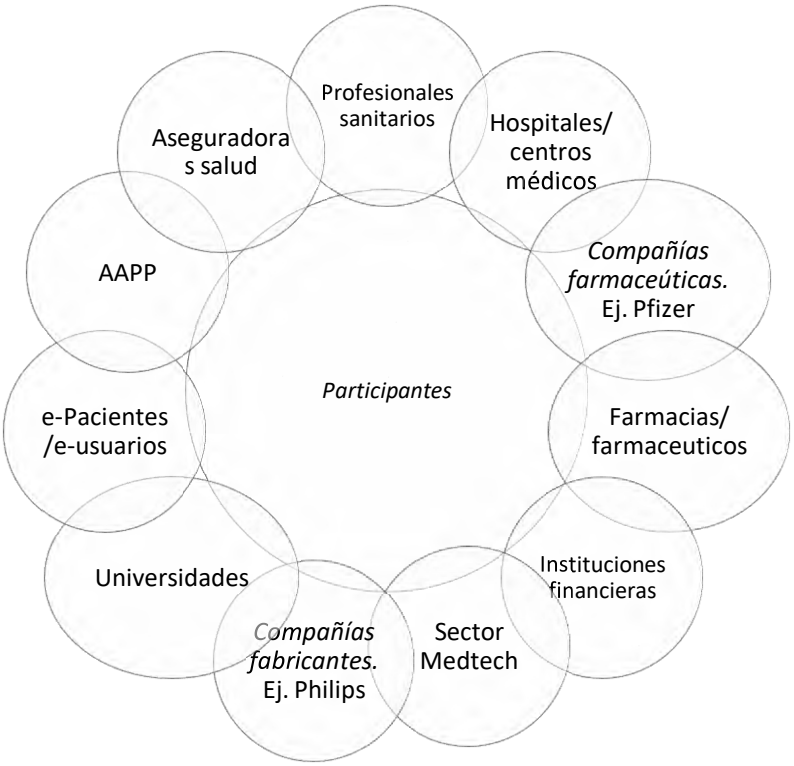


Image 54. Ejemplo de ecosistema de participantes en la Industria del Cuidado de la Salud. Fuente propia.

Gracias a este hipotético sistema de Blockchain se podrán realizar las siguientes acciones

- Acceso por parte del *e-paciente/e-usuario* a sus datos de salud desde cualquier sitio y dispositivo conectado a Internet, a través de una aplicación móvil o web.
- Acceso por parte de *otros actores (hospitales/centro médicos, profesionales sanitarios)* a los datos de las personas físicas interesadas, siempre que este acceso haya sido permitido explícitamente y de antemano bien por el paciente o bien por el centro médico productor del dato. Estos permisos pueden concederse o revocarse en cualquier momento y se almacenan en la blockchain.
- Acceso a datos anonimizados de forma agregada para uso en investigación por parte de los diferentes *universidades o centros investigadores* pueden participar si son incluidos en la blockchain privada para consultar datos. Los propios pacientes pueden otorgar y revocar el uso para investigación de sus datos, así como ver para qué fueron utilizados. Y ¿por qué no añadir Ong, asociaciones de enfermos, cooperativas, fundaciones, instituciones gubernamentales, asociaciones públicas autónomas tal y como mencionan SALUS COOP?[468]

Antes de desarrollar ideas sobre los sujetos, conviene señalar algo. *Blockchain* es un sistema descentralizado por naturaleza, y no encaja con el modelo de *dicotomía de*

[468] Vid https://static1.squarespace.com/static/57c55d71725e25ba4eb91756/t/58e533fb1b631bedcc67acad/1491416088875/Salus+coop.pdf pp. 17 (Ver cuadro).

responsable/encargado de tratamiento. No existe un sujeto que se responsabilice del mismo, al igual que no hay un responsable de internet. *Blockchain* es un protocolo no una tecnología, por lo que intentar determinar quién es el *responsable de tratamiento* resulta materialmente complicado. No obstante, intentaremos definir y perfilar posiciones jurídicas según el RGPD y haremos una interpretación tras el estudio jurídico detallado de las implicaciones de esta tecnología. *Prima facie*, un posible esquema podría ser el siguiente:

Tabla 18. Esquema de sujetos jurídicos en Blockchain de la Industria del cuidado de la salud. Fuente propia.

i. El responsable del tratamiento de datos en Blockchain

Responsable (art. 4.7. RGPD y 24 RGPD) es la persona física o jurídica que determina los fines y los medios para procesar los datos personales. Por lo que cualquiera que acceda a los datos almacenados en una cadena de bloques y haga tratamiento de datos (art. 4.2. RGPD) *según sus propios fines* se convierte en responsable de tratamiento. Pero las personas físicas (o empresas) que ingresan datos personales en *Blockchain* fuera de una actividad profesional o comercial, no son responsables (art. 2 RGPD). Por tanto, ¿p*odríamos considerar a los participantes como responsables del tratamiento*?[469] Sí, serán responsables cuando los participantes deleguen decisiones sobre los detalles técnicos y organizativos del tratamiento de datos a todos los nodos, mineros y

[469] Por tanto, *¿podríamos considerar al usuario/e-paciente de la plataforma eHealth (titular de datos) como responsable del tratamiento?* Sí. Pero atención, las personas que no estén relacionadas con una actividad profesional que ingresen datos personales en una cadena de bloques estarán exentas de pertenecer a esa figura de acuerdo con la exclusión de *"actividad puramente personal o doméstica"* (art. 2 RGPD). Pensemos por ejemplo, en el caso de que un usuario de eHealth que realiza "consultas" (ver definición de tratamiento de datos) en la cadena de bloques de otros usuarios para informarse sobre síntomas similares.

desarrolladores. Pensemos de igual modo, que en los sistemas de *blockchain* permisionados -como los que nos centramos en este trabajo-, los empleados como médicos o investigadores que realizan el tratamiento de los datos personales en su organización –hospitales o instituciones privadas de investigación- lo hacen en cumplimiento de las funciones que éstas ejercen como responsables del tratamiento.

Además, se puede dar que el tratamiento se lleve a cabo una asociación de participantes en una *blockchain* donde todos se considerarían corresponsables (Art. 25 RGPD). En ella se deberán *definir las obligaciones y responsabilidades de cada uno* respecto del cumplimiento del RGPD. Los titulares de datos personales (pacientes y consumidores) tienen que saber a qué entidad acudir para solicitar el ejercicio de sus datos. También, hay que tener en cuenta que no todos los participantes son usuarios igualmente de "empoderados", ya que como podemos ver, participan *hospitales*, *compañías multinacionales de tecnología y del sector pharma*, *pacientes*, etc. con capacidades y poder de decisión diferentes. Este poder de decisión respecto a los medios varía[470], por ejemplo, respecto al software instalado para el funcionamiento del sistema de DLT o de *blockchain*. No obstante, corresponde al usuario[471] de *blockchain* que actué como responsable del tratamiento, asegurarse de que la plataforma de *blockchain* cumple la normativa en materia de protección de datos personales.

Y por otro lado, *¿cómo se considerarían a los nodos (validadadores) y mineros?* Sólo si tienen un papel más activo se les consideraría "responsables del tratamiento". Esto ocurrirá cuando decidan sus propios fines, el hardware y el software[472].

Como se puede ver no resultará fácil identificar y diferenciar a los sujetos jurídicos en esta tecnología. En todo caso, en la evaluación conjunta habrá que centrarse en si los propósitos y medios son determinados por más de una parte. La práctica muestra que no todos los responsables lo son por igual .

[470] Este desequilibrio se ve reflejado también en las relaciones entre proveedores cloud y clientes cloud, sobre todo, con los pequeñas y medianas empresas (Ver Cap. de *cloud computing*).

[471] Por ejemplo, en blockchain públicas como la de la propia Bitcoin. Ver más info: www.bitcoin.org

[472] Por ejemplo, podrían compararse con un SWIFT o *servicio de mensajería financiera* que facilita las transferencias internacionales donde se procesan datos personales como nombres de los pagadores y de los beneficiarios. El GT29 consideró que SWIFT debería considerarse como responsable dada la autonomía y el margen de maniobra con la que actúa (al decidir localización del *data center*, sobre el desarrollo y la comercialización, etc.). En cambio, la AEPD, en su resolución 27 de julio de 2007, llegó a una conclusión contraria alcanzada en el GT29, al señalar que SWIFT actuaba como encargada de tratamiento y las entidades financieras eran responsables de la información en relación con los mensajes de pago que envían a través de la red Swift, y debían cumplir con el derecho de información de sus clientes.

ii. El encargado del tratamiento de datos en Blockchain

Tengamos en cuenta que el tratamiento de datos se puede producir por la intervención de los usuarios, nodos y mineros cuando envían, verifican y almacenan o registran las transacciones. Cuando hablamos de tratamiento en *Blockchain*, hemos dicho anteriormente, que puede ser "procedimientos automatizados" como el "registro" o la "difusión" o "cotejo" o "cualquier forma de interconexión".

Recordemos que el *encargado*, es cualquier persona física o jurídica que trata los datos personales en nombre del responsable (art. 4.8 RGPD) o también se define[473] como la persona física o jurídica, autoridad pública, servicio u otro organismo que presta un servicio al responsable que conlleva el tratamiento de datos personales por cuenta de éste. El encargado debe cumplir con las instrucciones de quien le encomienda un determinado servicio, respecto al correcto tratamiento (automatizado o no) de los datos personales a los que pueda tener acceso como consecuencia de la prestación de este servicio. Dicho esto se considerarán encargados de tratamiento a:

a. Los nodos y mineros.

- *Cuando los nodos ejecutan las instrucciones* del responsable *y verifican* que la transacción cumple con los criterios técnicos, por ejemplo, un formato y un cierto tamaño máximo, y que el participante tiene capacidad para realizar su transacción. En este caso, se podrían tratar de los mineros, y se les podría considerar como *"full nodes"*[474]. Por tanto "sólo algunos tipos de nodos descargan toda la cadena de bloques y contribuyen a validar y apoyar el libro mayor compartido, y el nivel de participación de en el tratamiento de los datos varía en función del algoritmo de consenso y en función de el nivel de apertura de la configuración de la cadena de bloques" (Giannopoulou, 2018, 9)[475].
- *Cuando los nodos tienen un papel poco activo* -equiparable a los proveedores cloud- se les consideraría "encargados de tratamiento" puesto que realizar acciones mencionadas por cuenta del responsable, si se puede decir así. Suele tratarse, en estos casos, de *nodos,* y no de mineros. En el Reglamento europeo, el

---

473 http://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/Guia-encargado-del-tratamiento-RGPD-CAST.pdf

474 No obstante, no es lo mismo. Los mineros procesan bloques y los nodos completos verifican si las transacciones que han sido empaquetadas en el bloque por los mineros son todas válidas. Algunos pueden ejecutar un nodo completo sin ejecutar el software de minería". Para más info sobre el debate existente ver foro en : https://bitcoin.stackexchange.com/questions/59220/what-is-the-difference-between-a-miner-and-a-full-node

475 Giannopoulou, A.; Ferrari, V. (2018) . Distributed Data Protection And Liability On Blockchains. *INTERNET SCIENCE. 5th International Conference, INSCI 2018*. St.Petersburg, Russia, October 24-26, Proceedings, Vol. 2. Workshops. Pág. 9.Recuperado de https://pure.uva.nl/ws/files/31868271/SSRN_id3316954.pdf

legislador no previó que los nodos individuales o mineros individuales son incapaces de validar por sí solos ya que requieren del consenso y las normas incorporadas.

b. Los proveedores de plataformas de Blockchain[476].

Las plataformas proveedoras de blockchain pueden dar soluciones tecnológicas de blockchain a pacientes (pensemos en asociaciones de pacientes o consumidores de servicios e-Health); proveedores de salud (hospitales públicos o privados, médicos, etc.); pagadores (organizaciones farmacéuticas o tecnológicas); centros de investigación (pública o privada); vendedores y socios (industria farmacéutica y terceros que comprar los datos). Recordemos que hablamos de blockchain cerradas y permisionadas dirigidas a un grupo concreto de participantes y respecto a los medios que utilizarán serán las herramientas que ellos mismos hayan previsto. Un ejemplo de proveedor de blockchain en el ámbito de la salud, a mi modo de ver, sería *HSBlox*:

Imagen 55. Pantallazo de HSBlox. Fuente: HSBlox[477]

Así por ejemplo, es llamativo que fuera de la UE, en China (Administración del Ciberespacio de China, CAC), haya regulación[478] expresa (con fecha del 15 de febrero de 2019) respecto a los proveedores tecnológicos y su posición jurídica. Por ejemplo, se puede encontrar definición de los proveedores blockchain como aquellas "*entidades o nodos* que proveen servicios de información al público y soporte técnico a través de dicha tecnología en computadores de escritorio o aplicaciones móviles". Pero lo más significativo es el deber de transparencia que se les obliga. Por un lado, a través de un registro público o la estipulación de acuerdos de servicio con los clientes blockchain aclarando derechos y obligaciones de ambas partes. Además, la CAC, el 30 de marzo de 2019, ha publicado una lista con 197 proveedores blockchain, "entre las compañías aprobadas, se encuentran Baidu Blockchain Engine (BBE), Alibaba Cloud Blockchain-

[476] Ver https://hsblox.com/ como ejemplo de plataforma proveedora de blockchain de eHealth.
[477] Ver https://hsblox.com/ como ejemplo de plataforma proveedora de blockchain de eHealth.
[478] Vid. https://www.coincrispy.com/2019/01/10/censor-chino-aprueba-regulacion-blockchain/;ver también el Reglamento de la CAC en http://www.cac.gov.cn/2019-01/10/c_1123971164.htm

as-a-Service (BaaS), Tencent TBaaS (TBaaS) y la plataforma BaaS, propiedad de JD.com" [479].

c. Los desarrolladores de plataformas.

Se puede decir que aunque "establecen el diseño del código y gobiernan los libros distribuidos" (Zetzsche, 2017)[480] tienen también la capacidad técnica para determinar *cómo se almacenan los datos, validarlos, almacenarlos y procesarlos por los nodos de las redes*. Sin embargo, están atados al consenso de la red considerando ya que para que puedan actualizar o modificar el protocolo con éxito, la red de nodos de validación *debe demostrar su acuerdo* con la opción indicada. Por lo tanto, mientras los desarrolladores estén simplemente ejecutando lo que la mayoría del grupo de consenso esté conforme, no podrán ser considerados como responsables o partes interesadas reales en el proceso de toma de decisiones. Pueden ser desarrolladores de *Blockchain-as-a-service (BaaS)*.

d. Los desarrolladores de SC.

Cuando realizan tratamiento de datos personales en nombre del responsable, según la CNIL. Por ejemplo, pensemos en los programadores de *Hyperledger* para estos sistemas permisionados de *blockchain*, pensamos en actores con funciones de encargado de tratamiento, puesto que reciben instrucciones para realizar una aplicación permisionada. Podrían actuar en algunas ocasiones como encargados de tratamiento, y en otras, como subencargados de tratamiento (¿por qué no?). Es posible que mineros y nodos no autónomos en calidad de encargados subcontraten a otros actores que tendrán función de encargados. Por ejemplo, una empresa desarrolladora podría ser *Aeternity*.

iii. El subencargado del tratamiento de datos personales en Blockchain

Pensemos en los sub proveedores desarrolladores de *Blockchain-as-a-service (BaaS)*[481] como si fueran subproveedores cloud, como terceros que ofrecen la infraestructura de soporte a los destinatarios del tratamiento de datos para que ejecute el

[479] Vid. https://www.coincrispy.com/2019/04/02/regulador-china-companias-blockchain-aprobadas/?utm_medium=pushnotes; Ver también http://www.globaltimes.cn/content/1144347.shtml
[480] Zetzsche DA Buckley RP, Arner DW (2017). The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain, *University of New South Wales Law Research Series*. Law Working Paper Series, Number 2017-007. Recuperado de http://dx.doi.org/10.2139/ssrn.3018214
[481] Vid. https://www.coincrispy.com/2018/05/23/como-funciona-blockchain-as-a-service-baas/

minero y el nodo en el hardware del tercero. De hecho, ejecutan las instrucciones de la persona encargada de procesamiento cuando verifican que la transacción cumple con los criterios técnicos[482]. Estas plataformas permiten a empresas y usuarios abordar su uso sin tener necesariamente que asumir un desarrollo desde cero. Por tanto, deben establecer con el participante responsable un contrato que especifique las obligaciones de cada parte e incorporando las disposiciones del artículo 28 RGPD, tal y como realizarían un proveedor cloud con un subproveedor cloud (Ver capitulo correspondiente). Además, también se prevé la situación en la que los propios participantes responsables contratan estos servicios.

Visto todo ello, mostramos un cuadro comparativo como ejemplo para una mejor comprensión;

DIFERENCIAS		
Responsable Cliente Blockchain	*Encargado* Proveedor Blockchain	*Subencargado* BaaS
Reduce sus funciones de gestión de operatividad y mantenimiento al proveedor. Desarrolla el contenido por sí mismo. Ej. Como el cliente Hosting Cloud.	Deberá encargarse de la configuración, la conexión de los nodos y el complejo back-end en nombre del cliente. También tendrá la responsabilidad de que funcione correctamente su infraestructura y software y sobre todo, las *medidas de seguridad* concretas.	Es la creación soluciones basadas en la nube que permitan utilizar la cadena de bloques *como un servicio*. El usuario deberá pagar con un precio correspondiente por su capacidad de uso y su mantenimiento. https://nem.io/technology/

Tabla 19. Cuadro comparativo entre responsables, encargados y subencargados en Blockchain. Fuente propia.

iv. El titular de datos personales en Blockchain.

Serán los participantes que sean personas físicas, y no jurídicas, y podrán tener también la posición jurídica de responsable de tratamiento. El RGPD da a los individuos el control sobre sus datos personales; pero también asume que los actores claramente identificados

[482] Respecto a Blockchain as a Service (BaaS) según Allende, "algunas grandes compañías ofrecen servicios de blockchain en la nube. Algunos ejemplos son IBM especializada en Hyperledger Fabric, Amazon colaborando con Digital Currency Group, o Microsoft ofreciendo servicios de R3, Hyperledger Fabric o Quorum, entre otras. Estos servicios no solo consisten en almacenamiento de información, en este caso del blockchain, sino que las ventajas de este tipo de servicios son un aumento en la seguridad, la no necesidad de invertir en hardware y la posibilidad de un entorno más amigable con el que trabajar, pudiendo crear tu propio canal de blockchain sin necesidad de programar"

(o identificables) tienen control sobre el almacenamiento y tratamiento de datos , por lo tanto, son responsables de dicho control (Giannopoulou et al., 2018)[483].

La conclusión es que las obligaciones derivan de las calificaciones y roles legales de los diferentes actores (mantenimiento del registro, análisis de impacto, privacidad por diseño, notificaciones, etc.). Los participantes serían considerados responsables del tratamiento de los datos personales que envían a la plataforma de blockchain, ya que determinan los fines para ejecutar la transacción y los medios (red hyperledger) para elegir la plataforma. Además, delegarán decisiones sobre los detalles técnicos y organizativos del tratamiento de datos a todos los desarrolladores, nodos y mineros. Tengamos en cuenta que el RGPD no pretende regular las tecnologías sino los usos que hacen los actores en un contexto que involucra datos personales.

3.5.Obligaciones de los sujetos jurídicos

Ejemplos	
Responsable	Encargado
- Cliente Blockchain - Usuarios e-patient - Hospital/centros médicos	- BaaS (Proveedor Blockchain) - Empresa Farmacéutica - Centros de investigación

Tabla 20. Ejemplos responsables y encargados en blockchain en la Industria del cuidado de la salud.

Para continuar analizando a los sujetos jurídicos implicados y sus obligaciones seguiremos manteniéndonos en el modelo de blockchain privada y permisionada, alejándonos de las particularidades de las públicas y distribuidas[484].

En primer lugar, hablemos de las obligaciones de los responsables. Éstos aplicarán medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento en conforme al Reglamento. (Art. 24.1 RGPD). Se incluirán las oportunas políticas de protección de datos (art. 24.2 RGPD) y además será de considerar incluir como elementos de demostración de cumplimiento la adhesión a códigos de conducta o la tenencia de un mecanismo de certificación (Art. 24.3 RGPD).

Para cada plataforma, los responsables de tratamiento deberán establecer con los encargados de tratamiento un *contrato de encargo (*art. 28 RGPD) donde se determinen

[483] No obstante, no siempre tiene porque ser responsable de tratamiento. Una persona física que vende sus datos personales de salud a una compañía de Industria Farmacéutica y ésta le paga en una criptomoneda concreta se trataría de una actividad sujeta en el art. 2 RGPD de uso doméstico. Solo si lo hiciera en el marco de una actividad comercial o profesional se le podría considerar responsable de tratamiento.

[484] Parece complicado pensar cómo se podría cumplir estas obligaciones en el caso de *blockchain públicas y distribuidas* puesto que un gran número de participantes, nodos y mineros tendrían que celebrar múltiples contratos.

responsabilidades, en particular, cuestiones cómo se tratarán los datos, el contenido, la duración, la naturaleza y la finalidad del tratamiento. Pero además, si tenemos en cuenta nuestro escenario plural, los *corresponsables*, participantes emisores y destinatarios, deberán determinar sus responsabilidades de cumplimiento en un acuerdo (art. 26 RGPD). Para estos casos, podríamos tomar como recomendación lo que señala la CNIL. Se refiere a la posibilidad de que los participantes creen una persona jurídica en forma de Asociación u optar por identificar a un participante que está tomando decisiones para el grupo y designarlo como el responsable. De lo contrario, se podría considerar que todos los participantes tienen una responsabilidad de conformidad con el artículo 26 mencionado y, por lo tanto, deberían definir, las obligaciones de cada uno para garantizar el cumplimiento de la normativa. Y es que además, es necesario que las personas físicas sepan a qué entidad recurrir para ejercer sus derechos y las autoridades de control nacionales que les corresponderían para ejercer su derecho de tutela. En verdad, lo más factible en la práctica sería *el establecimiento de términos y condiciones* de forma estándar donde se obtenga el consentimiento expreso por cada primera vez que el participante entra en la interfaz. (¿Técnicamente será posible?)

Anteriormente, el regulador (Convenio 108) no sospechaba que fueran frecuentes escenarios con corresponsabilidad, hecho que no se regula hasta la llegada de la UE. El GT29 (Dictamen 1/2010) [485], en su intención de dar luz a esta cuestión ofrece orientación sobre la aplicación de este concepto a "sistemas complejos con *múltiples actores*, en los que *muchos escenarios* involucran a responsables y encargados, solos o en conjunto, con diferentes grados de autonomía y responsabilidad". Según este grupo de trabajo, "puede afirmarse que la *responsabilidad solidaria* de todas las partes debe ser considerado como un medio para eliminar las incertidumbres, y por lo tanto sólo en la medida en que sea una asignación alternativa, clara e igualmente efectiva de obligaciones y responsabilidades no han sido establecidas por las partes involucradas o no se derivan claramente de circunstancias fácticas". En la evaluación conjunta habrá que centrarse en si los propósitos y medios son determinados por más de una parte. La práctica muestra que no todos los responsables lo son por igual[486] .

[485] *Supra cit.* Pág. 24.

[486] Además, tendrá que cumplir el art.25 RGPD, en caso de que se trate de una blockchain pública para evaluar que los riesgos para las personas físicas con el impacto de esta tecnología sobre su protección de datos y privacidad. Pero además, el responsable del tratamiento debe elegir un encargado del tratamiento que ofrezca *garantías suficientes* respecto a la implantación y el mantenimiento de las medidas técnicas y

Después de todo lo mencionado, me surgen algunas cuestiones;

- ¿Cómo va ejercer el deber de diligencia el usuario (participantes responsables) sobre los hospitales o centros médicos (nodos que almacenan datos y encargados de tratamiento)?
- ¿Cuándo se deberá hacer EIPD, en las blockchain públicas? ¿qué medidas técnicas y organizativas deberán incluirse para asegurar la confidencialidad? (Ver aptado soluciones)
- ¿Cómo ejecutar el art.13 RGPD del deber de información? ¿en las políticas de privacidad?¿en un interfaz?
- Teniendo en cuenta que los participantes son responsables de tratamiento dentro de un consorcio ¿los usuarios de eHealth decidirán los fines y los medios para el tratamiento en blockchain?
- ¿Es posible que un participante sea responsable y encargado? Pensemos en un hospital privado que es responsable de tratamiento puesto que determina los medios y los fines del tratamiento.
- ¿Cómo funcionaría un *canal privado* dentro del propio consorcio? Pensemos en un canal entre hospitales, sector Medtech, e-pacientes y usuarios, y universidades; donde los cuatro deciden tratar determinados datos y aislarlos del resto, además de los fines de tratamiento y los medios, donde las compañías farmacéuticas y compañías fabricantes pudieran ser encargados de tratamiento en tanto que reciben instrucciones de la forma del tratamiento de las cuatro primeras.

En segundo lugar, *hablemos de las obligaciones del encargado de tratamiento en blockchain.* El encargado (por ejemplo, el médico puede realizar todos los tratamientos (consultas de datos de salud) que el responsable del tratamiento (por ejemplo, el paciente o usuario eHealth) le haya encomendado formalmente. El encargado del tratamiento en ningún caso puede variar las finalidades y los usos de los datos ni los puede utilizar para sus propias finalidades. El contenido de las obligaciones del *contrato de encargo de tratamiento* que tienen que tener responsables y encargados de tratamiento tienen que referirse al art. 28.3 RGPD concretamente a que (APDCAT[487]). Además, el art. 28.4 establece y extiende esas obligaciones a los subproveedores debiendo existir dicho acuerdo formal entre ambas partes.

Además habrá que tener en cuenta que

organizativas apropiadas, de acuerdo con lo establecido en el RGPD, y que garantice la protección de los derechos de las personas afectadas. Existe, por tanto, un deber de diligencia en la elección del encargado. El Considerando 81 del RGPD prevé que el encargado del tratamiento debe ofrecer suficientes garantías en lo referente a conocimientos especializados, fiabilidad y recursos, con vistas a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del Reglamento, incluida la seguridad del tratamiento.

[487] *Supra cit.*

A continuación, sirviéndonos de esta guía se ha realizado una posible plantilla:

EJEMPLO MODELO DE ENCARGO DE TRATAMIENTO

1. Objeto y finalidad del encargo del tratamiento

Mediante las presentes cláusulas se habilita a la (entidad proveedora blockchain/desarrolladora SC, etc.), encargada del tratamiento, para tratar por cuenta del (hospital/aseguradora/universidad, etc.), responsable del tratamiento, los datos de carácter personal necesarios para prestar el servicio de…… . .

El tratamiento consistirá en: *(descripción detallada del servicio)*

Concreción de los tratamientos a realizar:

☐	Recogida	☐	Registro
☐	Estructuración	☐	Modificación
☐	Conservación	☐	Extracción
☐	Consulta	☐	Comunicación por transmisión
☐	Difusión	☐	Interconexión
☐	Cotejo	☐	Limitación
☐	Supresión	☐	Destrucción
☐	Comunicación	☐	Otros ……

2. Identificación de la información afectada

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, la entidad/órgano entidad proveedora blockchain/desarrolladora SC, etc.), responsable del tratamiento, pone a disposición de la entidad (hospital/aseguradora/universidad, etc.), encargada del tratamiento, la información que se describe a continuación:

- HCE, datos y registros de wearables, testimonios de información de personal de salud, etc.

Categorías de personas interesadas: *ciudadanos / usuarios / clientes / trabajadores / pacientes / menores / personas discapacitadas / … (indicar la opción que proceda).*

3. Duración

El presente acuerdo tiene una duración de.....[488]

4. Obligaciones del encargado del tratamiento

[488] En algunos casos, en particular determinados casos sometidos al derecho administrativo (convenios, contratos de gestión de servicios públicos, etc.), la duración del encargo puede estar limitada por la duración establecida por la legislación vigente para la prestación de servicios.

El encargado del tratamiento y todo su personal se obliga a:

a) Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

b) Tratar los datos de acuerdo con las instrucciones documentadas del responsable del tratamiento.

Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediatamente al responsable.

c) Incorporar los tratamientos que lleva a cabo en ejecución de este contrato a su registro de actividades del tratamiento efectuadas por cuenta de un responsable, con el contenido del artículo 30.2 del RGPD[489].

d) No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles.

El encargado puede comunicar los datos a otros encargados del tratamiento del mismo responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación.

Si el encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

e) Subcontratación

> "Se autoriza al encargado a subcontratar con la empresa (ej. *MET /HYPERLEDGER)* las prestaciones que comporten los tratamientos siguientes:
>
> Para subcontratar con otras empresas, el encargado debe comunicarlo por escrito al responsable, identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo de ……[490].
>
> El subcontratista, que también tiene la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del tratamiento y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación, de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones."

f) Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice su objeto.

---

[489] La obligación indicada en el artículo 30.2 del RGPD no se aplicará a empresas ni organizaciones que ocupen menos de 250 personas salvo que concurra alguna de las siguientes circunstancias:

a) Si es probable que exista un riesgo para derechos y libertades de los sujetos.
b) Si el tratamiento no es ocasional.
c) Si incluye categorías especiales de datos (art 9 RGPD) o infracciones y condenas penales.

Si concurre alguna de estas circunstancias el encargado deberá incluir en el registro los tratamientos en los que concurran.

[490] Se recomienda establecer un plazo para que pueda oponerse.

g) Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a seguir las instrucciones del responsable, a respetar la confidencialidad[491] y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

h) Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

i) Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

j) Asistir al responsable del tratamiento en la respuesta al ejercicio de los derechos de:

1. Acceso, rectificación, supresión y oposición
2. Limitación del tratamiento
3. Portabilidad de datos
4. A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles)

"El encargado del tratamiento debe resolver, por cuenta del responsable, y dentro del plazo establecido, las solicitudes de ejercicio de los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, en relación con los datos objeto del encargo"[492].

k) Derecho de información.

"El encargado del tratamiento, en el momento de la recogida de los datos, debe facilitar la información relativa a los tratamientos de datos que se van a realizar. La redacción y el formato en que se facilitará la información se debe consensuar con el responsable antes del inicio de la recogida de los datos".

l) Notificación de violaciones de la seguridad de los datos.

El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de……..[493], y a través de……, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia. No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

m) Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

n) Dar apoyo al responsable del tratamiento en la realización de las consultas previas a la autoridad de control, cuando proceda.

o) Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.

p) Implantar las medidas de seguridad siguientes:

q) Las medidas de seguridad que se deriven de la aplicación de[494] ……

[491] Si existe una obligación de confidencialidad de naturaleza estatutaria deberá quedar constancia expresa de la naturaleza y extensión de esta obligación.

[492] A pesar de que la delegación en el encargado es una decisión que corresponde al responsable, resulta especialmente recomendable en aquellos supuestos en que los datos se traten exclusivamente con los sistemas del encargado.

[493] El plazo debe ser inferior a 72 horas en cualquier caso.

[494]Indicar el código de conducta, el sello, la certificación u otro estándar donde están definidas las medidas aplicables, como sería el caso del Esquema Nacional de Seguridad (ENS) para las entidades

En todo caso, deberá implantar mecanismos para:

a) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

b) Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

c) Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.

d) Seudonimizar y cifrar los datos personales, en su caso.

También debe adoptar todas aquellas otras medidas que, teniendo en cuenta el conjunto de tratamientos que lleva a cabo, sean necesarias para garantizar un nivel de seguridad adecuado al riesgo.

La documentación relacionada con la gestión de los riesgos, incluyendo el resultado de las auditorías periódicas que se realicen, puede ser solicitada en cualquier momento por el responsable del tratamiento.

r) Designar un delegado de protección de datos y comunicar su identidad y datos de contacto al responsable.

s) Destino de los datos.

"Destruir los datos, una vez cumplida la prestación. Una vez destruidos, el encargado debe certificar su destrucción por escrito y debe entregar el certificado al responsable del tratamiento. No obstante, el encargado puede conservar una copia, con los datos debidamente boqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación."

3.6. Respecto a la privacy by design / by default

En primer lugar, hablemos protección de datos por diseño y defecto como principios y no como derechos individuales absolutos. Implican que el responsable tendrá que implementar las medidas técnicas y organizativas adecuadas, como la pseudonimización o la minimización de datos desde el momento inicial, antes incluso que el desarrollo de los whitepapers. Los arquitectos de sistemas blockchain o desarrolladores de software deberán tener en cuenta este principio desde el momento inicial del proyecto y la transparencia permitiendo que el titular de datos pueda controlar su tratamiento de datos, además de facilitar al cliente (responsable de tratamiento) la creación y mejora de funciones de seguridad (Art. 78 RGPD). El consejo más seguro para los desarrolladores de blockchain es que los *datos transaccionales* nunca deben almacenarse dentro de un blockchain. Con respecto a las *claves públicas*, se deben adoptar las soluciones de gestión de riesgos necesarias y se deben realizar evaluaciones de impacto de protección de datos detalladas (Art.35 RGPD)[495].

---

definidas en el artículo 77.1 LOPDGDD y las empresas o fundaciones vinculadas a estas entidades (D.A. 1a LOPDGDD).

[495] Parece obvio que el legislador tenían en mente modelos centralizados basados en la tecnología de recopilación, almacenamiento y tratamiento de datos que no se pudieran transponer fácilmente a bases de datos descentralizadas y distribuidas. Por ejemplo, la autoridad de control francesa CNIL recomienda a

3.6.1. Para blockchain públicas[496].

i. Solución Zcash: Argumentos sucintos de conocimiento[497].

BUTERIN[498] señala el funcionamiento de esta técnica en casos de propiedad de token digitales; "y es que para tener un sistema de token digital en funcionamiento, "no es necesario tener cuentas y saldos visibles –al público-; de hecho, todo lo que se necesita es una forma de resolver el problema del *doble gasto*: si tiene 100 unidades de un activo, debería poder gastar esas 100 unidades una vez, pero no dos. Las cuentas en este esquema se convierten en uso único: se crea una *cuenta* cada vez que se envían los activos y la cuenta del remitente se consume por completo. Si no se desea consumir completamente una cuenta determinada, simplemente debe crear dos cuentas, una controlada por el destinatario y la otra con el *cambio* restante controlado por el remitente. Este es esencialmente el esquema usado por Zcash".

Imagen 56. Esquema de Zcash. Fuente: https://www.blockchain.com/explorer

---

los actores que cuando implanten proyectos tecnológicos planteen el protocolo blockchain en lugar de otras alternativas tecnológicas.

[496] Pensemos en nuestro caso práctico y HIT Foundation para poder aplicarlo a un modelo de blockchain abierto como ese. Aunque las blockchain públicas con transacciones financieras no son objeto principal de estudio de este trabajo, conviene mencionar como funciona soluciones de privacidad para este tipo de blockchain. Las transacciones de pago *bitcoin* consiste en una dirección de origen, una dirección de destino y un monto de pago. Estas transacciones se agrupan en *bloques* y se almacenan en un libro mayor descentralizado denominado *cadena de bloques*. Debido a que la cadena de bloques es pública, cualquier persona puede ver el historial de todas las transacciones, a través del software *Bitcoin* o visitando cualquier servicio de monitoreo de cadenas de bloques. Si bien las direcciones no están vinculadas explícitamente a las identidades reales de los usuarios, varios trabajos recientes han demostrado que la cadena de bloques puede extraerse para obtener información sobre los hábitos de consumo de los usuarios.

[497] Vid. https://eprint.iacr.org/2013/507.pdf
[498] Vid. https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/

3.6.2. Para blockchain privadas: canales privados, hash, anonimización por capas o computación multipartita segura.

Se puede proteger la privacidad utilizando tecnología blockchain a través de diferentes métodos. Deberán valorarse estos métodos antes de diseñar la solución blockchain, a fin de determinar cuál responde mejor a los objetivos planteados y al modelo de negocio de la entidad – teniendo especialmente en cuenta la importancia de evitar desnaturalizar las principales características de la tecnología blockchain.

a. Canales privados.

Son vías de transmisión de información creadas por dos o más nodos que quieren compartir información en privado dentro la red blockchain, es decir, sin que los demás nodos sepan qué contenido comparten. Los datos que se comparten a través de los canales privados deben cifrarse. En este caso, los nodos A y B de la red blockchain dispondrán de esta clave y serán también los encargados de su custodia. Al cifrarse, cuando los nodos A y B decidan eliminar o rectificar alguna información dentro del canal privado, ejercitarán sus derechos- por ejemplo, revocación del consentimiento o limitación temporal del almacenamiento- conforme al RGPD, únicamente tendrán que eliminar la clave de descifrado de los datos personales en cuestión. Por tanto, los datos cifrados permanecen pero el hecho de haber eliminado la clave conlleva que los todos los nodos, incluidos A y B no puedan visualizar la información. [499]

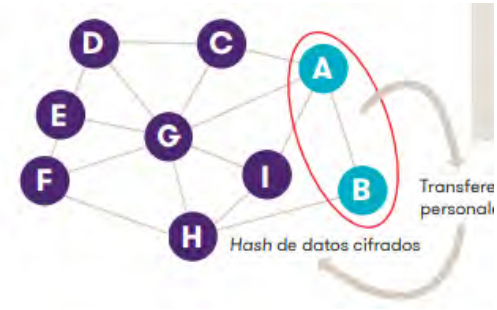


Imagen 57. Ejemplo de canal privado A y B. Fuente: GrantThornton

b. Hash con mayor protección de cifrado o "hash con salt".

[499] Vid. https://www.grantthornton.es/globalassets/___spain___/folletos/rgpd-y-blockchain-final.pdf

Los datos pseudoanonimozados permiten la identificación de los interesados en ciertos supuestos, por ello, puede ser necesario reforzar los hashes[500] y posibilitar la anonimización. Se entiende por *"salt"* un conjunto de valores aleatorios que se añaden al hash del dato personal en concreto, dificultando de esta forma la identificación del propietario de dicho dato. El GT29 señalan los tres aspectos clave que deben analizarse para verificar que la anonimización es correcta:

- Singularización: ¿es posible extraer de un conjunto de datos algunos registros que identifiquen a una persona física?
- Vinculabilidad: ¿es posible vincular como mínimo dos registros de un único interesado o grupo de interesados?
- Inferencia: ¿es posible deducir con una probabilidad significativa el valor de un atributo a partir de los valores de un conjunto de otros atributos?[501]

c. ***Anonimización por capas.***

Consiste en que el responsable, una vez anonimizados todos los datos que puedan servir para reidentificar a las personas, remite la información a su legítimo destinatario, quien decide realizar una segunda anonimización con el ánimo de que sus procesos utilicen sus propios recursos de anonimización, con lo que sería más fácil imputar responsabilidades y adoptar de un modo más ágil las medidas pertinentes.

d. La computación multipartita segura.

Según BUTERIN[502], "el requisito de confianza en los participantes también es oneroso; tenga en cuenta que, como es el caso con muchas otras aplicaciones, los participantes tienen la capacidad de guardar los datos y luego se ponen de manifiesto en cualquier momento futuro de la historia. Además, es imposible decir que lo han hecho, por lo que es imposible incentivar a los participantes para que mantengan la privacidad del sistema; por esta razón, la computación multipartita segura es posiblemente mucho

[500] Un hash es un código que se obtiene tras aplicar un algoritmo especial a una cadena de texto. Es decir que si tenemos, por ejemplo, una contraseña 123secreto456 y le aplicamos un hash SHA-1 obtendremos el valor 04c6f29a901a600b6fc4bf08a0a942000c902b4f. Además, esto no es reversible. En algunos algoritmos, ocurre que dos o más palabras diferentes puede obtener el mismo hash como resultado.

[501] Vid. https://www.grantthornton.es/globalassets/___spain___/folletos/rgpd-y-blockchain-final.pdf
[502] Vid. https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/

más adecuada para blockchains privadas, donde los incentivos pueden provenir de fuera del protocolo que las cadenas públicas".

Por otro lado, existen soluciones como *Enigma*[503] combinan *el uso de blockchain con off-blockchain*[504]. Guy Zyskind (cofundador) explicaba que en esencia, Enigma *"es como una caja negra. Envías los datos que quieras, los utiliza en la caja negra y solo devuelve el resultado. Los datos como tales nunca se revelan, ni al exterior ni a los ordenadores que ejecutan esas computaciones con los datos".*

4. INCOMPATIBILIDADES CON RGPD Y APROXIMACIÓN A POSIBLES SOLUCIONES.

4.1.Respecto a la transparencia y la designación del responsable.

La propia estructura de blockchain hace complicado determinar quién es el responsable. El hecho de que los nodos que gestionan y administran la información estén tan dispersos hace difícil cumplir con dicha obligación recogida en el art. 4 RGPD. Es necesario que el sujeto de los datos personales conozca a quién dirigirse para efectuar sus derechos. El art. 5.1.a. RGPD establece que los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»).

4.2.Respecto al principio de minimización de datos personales.

En segundo lugar, conviene mencionar el *principio de minimización de datos* y su incompatibilidad con el RGPD, el cual exige que los datos personales se recopilen para fines específicos, explícitos y legítimos y que el tratamiento. Los datos una vez que son registrador permanecen con un carácter estable como "parte" de la cadena de bloques. Y es que los DLT están en continuo crecimiento, que aumentan y acumulan

[503] Vid. https://enigma.co/
[504] Guy Zyskind ; Oz Nathan ; Alex 'Sandy' Pentland . *ecentralizing Privacy: Using Blockchain to Protect Personal Data.* Recuperado de https://s3.amazonaws.com/enigmaco-website/uploads/pdf/ZNP15.pdf

datos adicionales con cada bloque de cadenas adicional (Finck, 2018)[505]. Resulta imposible implantar este principio puesto que cada nodo completo contiene una copia completa de cada blockchain y se agrega un nuevo bloque a la cadena completa anterior, esta disposición no se puede cumplir con respecto a las claves públicas. La única forma de garantizar el cumplimiento a este respecto sería reconocer técnicas específicas de manejo de claves, como fórmulas de cifrado particularmente sólidas o pruebas de conocimiento cero que cumplan con las normas RGPD.

4.3.Respecto al derecho de rectificación.

En tercer lugar, la obligatoriedad de satisfacer el *derecho de rectificación* del titular respecto a los datos personales inexactos teniendo en cuenta los fines de tratamientos sin demoras indebidas (Art. 16 RGPD). Entran en conflicto con la naturaleza de inmutabilidad de esta tecnología. No obstante, la capacidad de cumplir el RGPD depende del diseño de la plataforma. Así, las centralizadas pueden soportar mejor la reversibilidad y limitar la visibilidad de un registro a ciertos participantes, por lo que estarían en mejores condiciones para llevar a cabo los derechos de rectificación o cancelación. Pero para las abiertas y distribuidas, no está del todo definido como podrían los responsables de tratamiento (participantes, nodos o mineros) satisfacer los derechos de los titulares. Incluso si todos los participantes, nodos y mineros se consideraran responsable*s*, esto no necesariamente proporcionaría una protección efectiva para los titulares de datos personales *(Berberich y Steiner, 2016)*[506].

Cuando deban modificarse los datos, de acuerdo con el principio de exactitud, el responsable del tratamiento los modificará en la base de datos externa. El registro actualizado sustituirá al anterior registro de la base de datos externa y recibiendo un nuevo hash, que se almacenará en blockchain. El hash de los datos personales antiguos pasará a ser, nuevamente un número aleatorio carente de significado por no tener correspondencia con ningún dato de la base de datos externa.

---

[505] Fink, M. (2018). Blockchains y Protección de datos en la Unión Europea. *Der Juristiche Verlag Lexxion.* Vol. 4, No. 1. Pp. 17-35. Recuperado de https://edpl.lexxion.eu/article/edpl/2018/1/6/display/html

[506] Berberich, M., Steiner, M., (2017) "Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?", 2 Eur. Data Prot. L. Rev., 422.

La coordinación entre miles de nodos resulta muy complicada para acordar una nueva versión de la cadena de bloques o alterarla. Se pueden realizar técnicamente de varias formas que intentaremos explicar de la forma más fácil posible.

Se pueden, proporcionar por ejemplo a través de *enlaces*[507] (o por notificación suplementaria) a los datos que residen externamente a la misma, de esta manera el responsable satisfacería dicho derecho haciendo que esos datos sean inaccesibles. Se está investigando profundamente y contrarreloj en el ámbito técnico para posibilitar ejercer estos derechos. Pero comparto una duda ¿podría cumplir con este artículo el hecho de añadir datos que rectifiquen los datos agregados previamente sin modificar la entrada original? No parece ser la solución más adecuada pero sí lo sería la modificación de los datos almacenados fuera de la cadena. ¿Pero lo sería para todos los datos personales? No, sólo para los transaccionales (Cfr. Fink) y no con los datos referentes a las claves públicas. Ahora bien, este obligatoriedad está unida a la obligatoriedad de que el responsable comunique dicha rectificación que en el caso de las DLT estaría exenta su aplicación a los nodos dado a que serían imposible o requerirían un esfuerzo desproporcionado.

Sin embargo, en cambio, puede haber casos en los que no sea apropiado borrar los datos personales corrigiéndolos (aunque los datos sean incorrectos). Pensemos en un contrato firmado donde los datos son un medio de prueba. En estos caso podría ser preferible adjuntar una *declaración aclaratoria al contrato* de modo que siguiera sirviendo como prueba y los términos siguieran siendo exactos e inalterados. Sobre este terreno no hay nada escrito y requeriría de pronunciamiento de las autoridades de control y de los reguladores.

Y por otra, a través de la edición por bifurcación ("forks"). En ella tenemos que tener en cuenta que la mayoría de los nodos deben estar de acuerdo con un nuevo conjunto de reglas iniciales y, a continuación, actualizar el software utilizado para ejecutarse el Blockchain para que la mayoría de los nodos de una red Blockchain estén de acuerdo con el nuevo libro mayor. En la práctica puede ser muy costosa y compleja en su operación.

4.4.Respecto al derecho de acceso

[507] Guy Zyskind, et al., Descentralización de la privacidad: uso de Blockchain para proteger datos personales, *2015 IEEE Sec. talleres de privacidad* 180, 181 (2015).

En cuarto lugar, la obligatoriedad de satisfacer el *derecho de acceso* en el que el titular tiene el derecho de obtener la confirmación del responsable de si están siendo tratados sus datos o no (Art. 15 RGPD), donde podría solicitar información sobre el tratamiento, la categoría de datos, los destinatarios, la duración y si se existe una decisión automática incluyendo el perfilado. Pero además, los titulares tendrían derecho a ser informados sobre las salvaguardas (art. 15.2 RGPD) que se aplican cuando los datos se transfieren a terceros países, esto es de interés puesto que un nodo que valida un bloque dentro de la UE compartirá esa información con todos los nodos de la cadena sea cual sea la localización geográfica.

A quien predice que los sistemas DLT pueden ser diseñados de forma que el usuario tenga acceso a la clave pública y privada y, decidir además cuándo revela sus datos a terceros[508].

Hay que tener en cuenta algo muy importante: los responsables desconocen qué datos son almacenado en la cadena ya que sólo manejan la versión cifrada o hash del dato. De por sí es complicado que un titular contacte con los nodos, pero igual de complicado es que ese nodo pueda confirmar al titular que se está realizando tratamiento de datos o no. Por último, el art. 15.3 está relacionado con el derecho del titular a pedir copia de sus datos personales a los responsables, pero, ¿sería posible materialmente? Puede resultar complicado si los datos personales están pseudonimizados criptográficamente. La solución más adecuada sería el registro fuera de la cadena para los datos transaccionales pero sigue resultando inviable para los datos de las claves públicas.

Tampoco sería posible casar la obligación de la conservación limitada de los datos personales en el tiempo (art. 5.1. e RGPD) . Los datos personales se quedarán ingresados en las cadenas de bloques.

4.5.Respecto al derecho de supresión (o al olvido)

En quinto lugar, la obligatoriedad de satisfacer el *derecho del olvido* o al borrado de los datos personales que le conciernen al titular sin demora indebida es otra de las incompatibilidades. “Algunos creen que las blockchains públicas sin permiso no pueden

[508] Mainelli, M. Blockchain podría ayudarnos a recuperar el control sobre nuestros datos personales Recuperado de https://hbr.org/2017/10/smart-ledgers-can-help-us-reclaim-control-of-our-personal-data

ser compatibles con RGPD, y que las blockchains privadas podrían ser la respuesta a los problemas regulatorios de blockchain. Aun así, las blockchains privadas cuestionan el significado de lo que es una blockchain. No hay una respuesta simple" **(**M**.** Beedham, 2018)[509]. Dave Michels de la U.Queen Mary señaló que "para resolver estos rompecabezas de diseño, debemos utilizar soluciones creativas que respalden las normas de diseño"[510].

Por ejemplo, la compañía tecnológica Embleema[511] , respecto al derecho de supresión, establece lo siguiente en su web de políticas de privacidad:

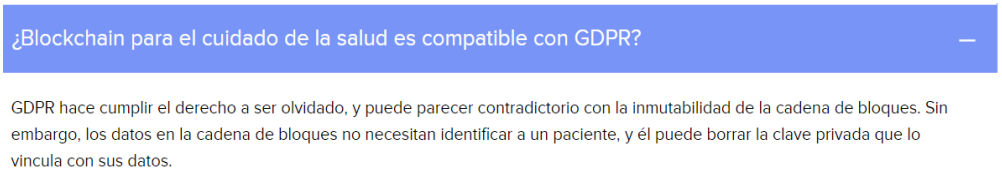


Imagen 58. Clausula de protección de datos referente al derecho de olvido Embleema. Fuente: Embleema.

Debe recordarse que el derecho a ser olvidado no es un derecho absoluto. Donde más problemas existirían tendrían que ver con las claves públicas[512]. La tecnología blockchain se podría agarrar a la exención de las *limitaciones técnicas*. Algunos autores, de hecho, consideran que la eliminación de la clave privada en un entorno supervisado podría constituir una eliminación para los fines del RGPD. A diferencia del borrado total, los datos cifrados seguirían existiendo en la cadena, pero solo podrían acceder a ellos el sujeto de los datos (a través de su control exclusivo de la clave privada) o

[509] Vid. https://thenextweb.com/hardfork/2018/12/14/blockchains-privacy-by-design-gdpr/

[510] Él cree que los *datos de la transacción se pueden cifrar* con una clave privada para generar un texto cifrado que se puede almacenar en la cadena de bloques de una manera inmutable. Si se quiere olvidar, eliminar y eliminar la clave hace que los datos de la transacción almacenados en el texto cifrado sean ilegibles, pero *no rompe la cadena de registros almacenados en la cadena de bloques*. Sin embargo, el problema es que esto crea un nuevo desafío de dónde y cómo almacenar estas claves privadas, en algunos casos puede llevar a un *punto de centralización*. Si este es el caso, desafía la noción de si la descentralización es la mejor opción para la aplicación dada de la cadena de bloques, devolviéndonos al cuadrado uno. Por supuesto, estas soluciones solo son aplicables para RGPD, otras naciones tendrán diferentes tomas en la regulación, por lo que abordar el cumplimiento de la cadena de bloques a nivel global es aún más difícil.

[511] Más info: https://www.embleema.com/faq/ para más info: https://www.embleema.com/wp-content/uploads/2018/10/GDPR-Data-Processing-Addendum.pdf (Ver pol. Privacidad).

[512] El artículo 17.2 RGPD establece que, "ante una solicitud de eliminación, el controlador de datos tendrá en cuenta la tecnología disponible y el costo de implementación y luego tomará los pasos razonables, incluidas las medidas técnicas, para informar a los controladores que están procesar los datos personales que el interesado ha solicitado el borrado por parte de dichos controladores de cualquier enlace, copia o replicación de dichos datos personales".

simplemente ya no se podría acceder a ellos. Algún autor[513] establece incluso que: "*la poda se puede utilizar para eliminar transacciones obsoletas* en bloques más antiguos que ya no son necesarios para la continuación de la cadena, pero la idea sigue siendo controvertida".

Otra opción, al margen de la poda, sería el uso *de "hash de camaleón"* para volver a escribir el contenido de los bloques en un DLT por las autoridades autorizadas bajo restricciones específicas con total transparencia y responsabilidad. Cuando deban eliminarse los datos personales, de acuerdo con los principios de legitimidad del tratamiento o limitación del plazo de conservación, el responsable del tratamiento eliminará los datos de la base de datos externa, mientras que el hash correspondiente permanecerá en blockchain. Al eliminar los datos correspondientes con este hash, éste se convierte en un número aleatorio sin correspondencia, de modo que la información almacenada en blockchain pasa a ser ininteligible y, por tanto, irrelevante.

Sin embargo, hay una serie de problemas con este enfoque según la autora *M. Fink*:

- Primero, si la llave de bloqueo se destruye o se pierde, la cadena vuelve a ser inmutable. Además, esta solución reintroduciría la necesidad de un tercero de confianza, como cuerpos especiales o árbitros, lo que a algunos les parecerá inaceptable, dado que podría decirse que anula el beneficio mismo de los DLT.
- En segundo lugar, los hashes de camaleón no pueden eliminar las copias antiguas de la cadena de bloques que aún contendrán la información redactada y los mineros también tienen la discreción de aceptar o no los cambios. Se debe enfatizar que las bifurcaciones duras, que se pueden usar para mutar blockchains en casos muy excepcionales, no son herramientas de cumplimiento RGPD viables. Los forks duros solo tienen sentido para el bloque extraído más recientemente, ya que todos los bloques subsiguientes se vuelven inválidos, por lo que todas las transacciones almacenadas en estos bloques tendrían que ser reprocesadas, lo que sería demasiado costoso independientemente del protocolo de consenso que se use y tomará una gran ventaja[514].

¿Cómo piensan los EEMM? *En Alemania[515], se a*cepta que los datos no se eliminan cuando el modo específico de almacenamiento hace esto imposible. En tales

[513] Palm, E.. *Implicaciones e impacto de la poda de transacción de blockchain.* (Tesis de maestría, Luleå University of Technology 2017). Recuperado de http://www.diva-portal.org/smash/get/diva2:1130492/FULLTEXT01.pdf

[514] Ateniese G. et al. (2017). Redactable Blockchain - or - Rewriting History in Bitcoin and Friends. *IEEE European Symposium.* Recuperado de http://ieeexplore.ieee.org/document/7961975/

[515] El art. 35.1 de la ley alemana de protección de datos establece: "Si en el caso de la eliminación no automatizada del procesamiento de datos fuera imposible o implicara un esfuerzo desproporcionado *debido al modo específico de almacenamiento* y si el interés del interesado en el borrado es mínimo, el interesado no tendrá el derecho de cancelación y el responsable no estará obligado a borrar datos

circunstancias, se tolera una "solución alternativa de no eliminar" limitando el tratamiento de los datos. Mientras una clave pública esté en la cadena de bloques, siempre será "procesada" en el sentido de que forma parte de la cadena de bloques a la que se han asignado nuevos bloques. Esto resulta interesante ya que muestra que el RGPD puede interpretarse en función de sus objetivos teniendo en cuenta las características tecnológicas en concreto. Pero, ¿esto significa que podemos justificar una posible exención a las obligaciones cuando hayan limitaciones técnicas que sean incompatibles con el RGPD? Desde mi punto de vista, la respuesta es negativa. Blockchain no será la última tecnología en aparecer (la computación cuántica está en camino) por lo que habrá que buscar soluciones técnicas disruptivas, dinámicas y creativas, además de promover una cultura de privacidad a la medida de los consorcios y partes interesadas donde se fomente la confianza, la transparencia y la seguridad.

4.5.1. Aproximación a soluciones: Off chain y side chain

i. OFF-CHAIN [516].

La inmutabilidad de la cadena blockchain es inherente a este tipo de plataformas y se debe principalmente a la criptografía, al árbol de *Merkle* y al algoritmo de consenso, pero se trata de una rigidez absoluta. Esta característica esencial choca con el RGPD de lleno por lo que se tornan necesarias soluciones -técnicas- que posibiliten su cumplimiento. Algunas las podemos encontrar en la eliminación de las claves de descifrado relevantes -dejando solo datos indescifrables en cadena- o almacenando los datos *fuera de cadena.* Últimamente se están realizando experimentos acerca de almacenamientos de información por separado sobre otro sistema con restricciones de control de acceso. Proteger datos y gestionar el almacenamiento en la cadena de bloques. Algunas soluciones usan solo un hash de datos personales, que sirve como punto de referencia y enlace a un "off-chain" con dicha base de datos con información personal. Por ejemplo, IPFS[517] y *Blockchain* puede ser una combinación perfecta ya que

personales de conformidad con el artículo 17 (1) del Reglamento (UE) 2016/679, además de las excepciones establecidas en el artículo 17 (3) del Reglamento (UE) 2016 / 679 (…)"

[516] Vid. https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf

[517] Vid. https://ipfs.io/

los datos de salud se podrían almacenar, incluso, en la propia cadena.

Imagen 59. Pantallazo de IPFS. Fuente: IPFS.

Solo el usuario con su propia clave privada puede ver los documentos. Si un usuario desea otorgar a otra persona el derecho de ver algunos registros específicos descifrados, pero no todos, se puede usar algo como una billetera determinista para obtener una clave diferente para cada documento.

ii. SIDECHAIN.

A diferencia de "fuera de cadena", que generalmente almacena la información elegida en un red tradicional, "cadena lateral" es una *blockchain paralela (ver imagen inf.)*. Estas cadenas laterales son independientes y si fallan o son hackeadas, no dañarán otras cadenas. Según *Adam Back y Gregory Maxwell*, hay limitaciones o vacíos[518] que la tecnología *blockchain* necesitaba corregir y cuya solución la pueden brindar las cadenas laterales como el riesgo de posible falla de alguno de los tantos componentes criptográficos de la cadena del Bitcoin, lo cual implicaría la pérdida total de su valor.

Las cadenas laterales efímeras se pueden *agregar a cualquier bloque*, en cualquier momento, sin afectar la integridad de la cadena de bloques. También pueden eliminarse sin interrupciones, lo que los hace ideales para su uso en aplicaciones que deben administrar una capacidad de almacenamiento limitada además de cumplir con el RGPD. Las cadenas laterales efímeras se pueden conservar durante el tiempo que sea necesario y se pueden eliminar de una cadena de bloques una vez que la aplicación ya no las necesita. Esta función puede ayudar a las aplicaciones de la cadena de bloque posibilitando al cumplimiento del artículo 17 RGPD de supresión de datos. El cumplimiento simplemente requeriría eliminar cualquier cadena lateral que contenga información del sujeto de los datos.

[518] Back, A. et al. (2014) *Enabling Blockchain Innovations with Pegged Sidechains*. Recuperado de https://blockstream.com/sidechains.pdf

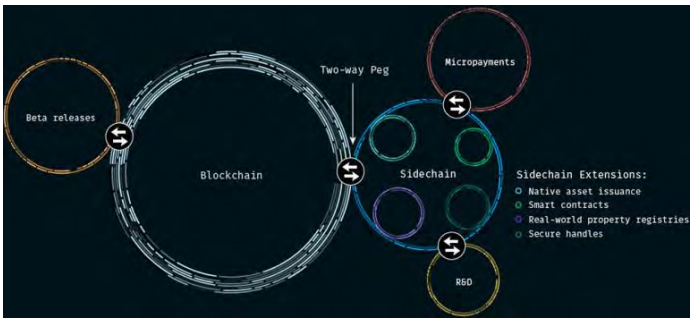


Imagen 60. Ejemplo de Sidechain. Fuente: https://academy.bit2me.com/que-son-las-sidechains/

4.5.2. Aproximación a soluciones: Uso de IA de middleware.

Normalmente se refiere a funciones de software diseñadas para reunir varias instancias y elementos interrelacionados de datos de blockchain. También puede abarcar *software* diseñado para combinar diferentes implementaciones de blockchain dentro de una interfaz unificada para facilitar su uso y (a menudo) como una ruta para lograr la escalabilidad. Un ejemplo de una plataforma de middleware de blockchain es *Omnitude,* la firma de tecnología británica se ha asociado con la plataforma de comercio electrónico de múltiples proveedores *CS-Cart* para incorporar *capacidades de identidad única* en la experiencia de venta minorista utilizando blockchain. U otro ejemplo es *Venzee* conocido por ser el primer middleware que prepara los datos antes de incorporarlos a la cadena de bloques. Pensemos por ejemplo, en redes de blockchain donde los usuarios se registran (con fotografías) este tipo de middleware podrían ayudar por medio de IA a borrar dichos datos personales [519]. Tal y como BUTERIN señala es importante tener presente que blockchain no resuelven problemas de privacidad y representa solo una solución de , autenticidad. Según él, "*colocar registros médicos en texto sin formato en una cadena de bloques es una idea muy mala. Sin embargo, pueden ser combinados con otras tecnologías que hacen ofrecer privacidad con el fin de crear una solución integral con el fin de proporcionar garantías de autenticidad*". BUTERIN señala que existen *soluciones parciales* para casos de uso específicos, y con frecuencia estas soluciones parciales ofrecen un alto grado de flexibilidad y son bastante diferentes de las que los desarrolladores están acostumbrados.

[519] Vid. https://martechtoday.com/venzee-launches-first-middleware-optimize-blockchain-bound-data-207051

Es necesario que se sustentan en el concepto de consorcio y círculo de confianza. Es necesario, para que Blockchain despegue en el área de la salud, que los participantes más relevantes (al menos pacientes, médicos, servicios de salud y farmacias) se adhieran y decidan dar un paso adelante en esa dirección. Conseguir que blockchain funcione cumpliendo la privacidad, no es un reto tecnológico, como un reto social, de espíritu de comunidad y de compromiso y de atrevernos a participar y empujar este cambio.

4.6.Respecto a la limitación del plazo de conservación.

La información que contiene una cadena de bloques, se mantiene de forma permanente para que esta pueda ser evaluada, actualizada y revisada con cada transacción que se realice. Pero el art. 5.3 RGPD establece que los datos personales deben mantenerse de tal forma que se pueda identificar a los interesados solo durante el tiempo necesario para los fines previstos. El desafío será poder eliminar los datos personales en el futuro, cuando concluyan los fines para los que fueron recogidos. Por tanto, si la información se mantiene después de cada transacción o tratamiento de datos, no es está cumpliendo lo previsto por el RGPD.

4.7.Respecto al equilibrio innovación tecnológica vs regulación.

Según *De Filippi*, concretamente, la innovación tecnológica plantea una variedad de desafíos, que la profesión jurídica tendrá que abordar que pueden clasificarse en cuatro fases:

i. proceso de digitalización de la información;
ii. automatización a los procesos de toma de decisiones;
iii. incorporación de las normas legales en el código la aparición de la regulación por código[520];
iv. codificación de la ley.

Dicho lo anterior, por tanto, nos encontramos con otra incompatibilidad será pretender un *equilibrio entre los derechos fundamentales y la promoción de la innovación* es todo un reto que afrontar por parte del legislador, y en concreto, lo será

[520] Con el despliegue generalizado de la red global de Internet, han surgido nuevas formas de regulación que dependen cada vez más del *soft law* (acuerdos contractuales y normas técnicas).

aplicar el RGPD en el contexto innovador tecnológico en continuo crecimiento. Esto se debe a que el RGPD surgió en un contexto y en una época de silos de datos centralizados donde el legislador no tuvo una visión de futuro previendo la gestión de datos descentralizados en tecnologías como la de blockchain o los sistemas DLT. Esta situación no es nueva ni única puesto que ha ocurrido con el Big Data. Como hemos visto en los párrafos anteriores, los derechos de rectificación y supresión no se pueden aplicar perfectamente al RGPD. Sólo en el caso de diseñar una plataforma de Blockchain desde el momento inicial teniendo en cuenta los derechos de los titulares, es decir, aplicando el principio rector de la privacidad desde el diseño y por defecto, se estaría aplicando correctamente la normativa. Estamos de acuerdo con que la solución idónea sería no almacenar los datos personales en la cadena de blockchain pero técnicamente se puede hacer en el caso de los datos transaccionales pero no en el caso de las claves públicas y firmar puesto que sin ellas no podría funcionar el sistema. Lo más necesario en todo caso sería una interpretación específica del RGPD que pudiera encajar con las particularidades del sistema.

En el RGPD, por su parte, en el considerando 6, el legislador señala que *la rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de datos personales y;* en el considerando 5 se señala el objetivo de la libre circulación de los datos personales. Y al mismo tiempo, el considerando 15 del Reglamento establece que *la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas actualizadas*. Ya en el artículo 173 del TFUE, la UE y los Estados miembros deben trabajar para lograr la competitividad de la UE, que incluye el *fomento de la innovación y el desarrollo tecnológico*. Somos conscientes que la máquina legisladora va por detrás y difícilmente alcanza el ritmo y la velocidad del desarrollo tecnológico, pero son posibles soluciones alternativas. Tampoco se puede concebir al derecho fundamental de protección de datos como un obstáculo para la innovación tecnológica; la coexistencia es posible y compatible. De hecho, se puede mantener que la tecnología blockchain y los sistemas DLT pueden suponer un contexto o marco de actuación para el cumplimiento del RGPD (véase el apartado de este capítulo) como complemento y aliado de éste último. Pensemos la aplicación principio rector de la privacidad por el diseño y por defecto por medio de desarrollo de técnicas tecnológicas.

De hecho, el propio SEPD establece que "las tecnologías avanzadas aumentan el riesgo para la privacidad y la protección de datos, también pueden integrar soluciones tecnológicas para una mejor transparencia y control para las personas cuyos datos se procesan". En este sentido, la autora Michele Fink[521], establece que "el RGPD podría estimular la innovación para que evolucione en una dirección que cumpla con estos importantes objetivos de política pública. Para que esto se materialice, no se puede evitar la discusión y el aprendizaje mutuo entre la industria y los responsables políticos".

En conclusión, si las cadenas de bloque se diseñan adecuadamente desde el momento inicial posibilitando el control de los titulares de los datos personales se podrán cumplir con el RGPD donde la interoperabilidad técnica-legal sea posible.

El investigador Christopher Millard[522] de la Universidad Mary Queen (2018), estableció que "Blockchain no es de ninguna manera la primera tecnología emergente en ser calificada como incompatible con la privacidad y otros principios legales fundamentales. Las aplicaciones de blockchain pueden ser disruptivas, pero eso no significa que no puedan diseñarse y desplegarse de una manera que cumpla con la ley".

[522] Queen Mary University of London (6 de noviembre de 2018). *Are blockchains compatible with data privacy law?*. Recuperado de https://www.qmul.ac.uk/media/news/2018/hss/are-blockchains-compatible-with-data-privacy-law.html

CAPÍTULO V. COMPLIANCE Y RESPONSABILIDAD EN MATERIA DE PROTECCIÓN DE DATOS PARA APLICAR EN LA INDUSTRIA DEL CUIDADO DE LA SALUD DIGITAL

SUMARIO: 1. LA GESTIÓN DE RIESGOS EN PROTECCIÓN DE DATOS. 1.1. La responsabilidad proactiva ("accountability"). 1.2. El análisis de riesgo. 1.3 .La evaluación de impacto.1.4.La gobernanza de datos. 2. AUTORREGULACIÓN. 2.1. Código - tipo de conducta. 2.2 .Autorregulación privada sectorial tecnológica. 2.3. Best practices corporativas. 3. CERTIFICACIÓN. 3.1. Sellos de privacidad. 3.2. Certificaciones técnicas. 4. HOMOLOGACIÓN. 5. COMPLIANCE. 5.1. Definición y características. 5.2. Responsabilidad, protección de datos y compliance. 5.3. Canales de denuncia ("whistleblowing"). 6. RESPONSABILIDAD SOCIAL EMPRESARIAL O CORPORATIVA. 7. EL RÉGIMEN SANCIONADOR. 7.1. El régimen sancionador en el RGPD. 7.2. El régimen sancionador en la LOPDGDD.7.3. EL DERECHO A INDEMNIZACIÓN Y RESPONSABILIDAD.

.

"El precio de la grandeza es la responsabilidad"

(Churchill)

1. LA GESTIÓN DE RIESGOS EN PROTECCIÓN DE DATOS.

1.1.La responsabilidad proactiva ("accountability")

La *responsabilidad* [523]es un concepto escurridizo y difícil que puede significar cosas muy diferentes y se refiere a "una esfera de deber u obligación asignado a una persona por la naturaleza de un cargo o función" (Barry, 1979)[524]. Por su parte, la *responsabilidad proactiva* (o *rendición de cuentas)*, por su parte, "va más allá de la responsabilidad porque no se limita a designar quién es responsable de una acción, sino

[523] La *"accountability"* proviene de la palabra latina ("*accomptare*") o ("*a cuenta*"), un prefijo utilizado en el sistema de préstamo de dinero desarrollado en la antigua Grecia y Roma. Podemos referirnos a diferentes tipos de responsabilidad proactiva (o rendición de cuentas), morales, administrativas, políticas, de gestión, de mercado, jurídicas o judiciales, profesionales. *Accountability* es la expresión traducida en inglés de "responsabilidad proactiva" o "rendición de cuentas. Responsabilidad y rendición de cuentas - aunque son sinónimos - resultan ser conceptos diferentes.

[524] BARRY, V. E., (1979) *Moral Issues in Business*, Belmont, CA. en CONVERSO, Domenico, The accountability of data controllers in relation to cloud providers, 2013. Recuperado de http://arno.uvt.nl/show.cgi?fid=131417

que también exige que la entidad que lleve a cabo la tarea pueda rendir cuentas, dar una razón o una explicación para justificar esa acción" (Comock, 2011)[525]. La rendición de cuentas es más que responsabilidad porque "implica un proceso de interacción transparente en el que el órgano externo busca la respuesta y la posible rectificación" (Bennet, 2010, 21)[526]. Concretamente, implican la presencia de normas y la existencia de una relación entre el foro o *"accountee"* (Bovens, 2006)[527] y el responsable *o "accountour"* que responde y rectifica. Pero además la rendición de cuentas; supone un *reconocimiento demostrable* de que se asume responsabilidad mediante políticas y buenas prácticas*;* significa contar con una plataforma que fomente la toma de decisiones responsables[528]; implica la posibilidad de sancionar a los que incumplan.

En el nuevo entorno digital, los individuos tienen el derecho a controlar efectivamente su información personal. La protección de datos es un derecho fundamental[529] en Europa y necesita ser protegido por ello. *La rendición de cuentas o "accountability",* llevada al ámbito de protección de datos, tomó forma hace más de 30 años, cuando fue adoptado como principio de protección de datos de la OCDE[530], "desde entonces, constituye *una herramienta legal* para exigir que la entidad responsable lleve a cabo las medidas necesarias para garantizar el cumplimiento de los principios de protección de datos personales" (Converso,12)[531].

---

[525] COMOCK, M., (2013). *Legal definitions of responsibility, accountability and liability,* Nursing children and young people, Aprile 2011 en CONVERSO, D., The accountability of data controllers in relation to cloud providers.

[526] BENNET, B., (2010) International privacy standards: can accountability ever be adequate?, *Privacy Laws & Business International Newletter*, p. 21. en CONVERSO, D., The accountability of data controllers in relation to cloud providers, 2013.

[527] POLLITT, C. (2003). The Essential Public Manager. London: Open University Press/McGraw-Hill en. BOVENS, M. Analysing and Assessing Accountability: A conceptual Framework, 2006, pág. 9 Recuperado de https://www.ihs.ac.at/publications/lib/ep7.pdf

[528] Ver Hunton & Williams LLP (2010) Demonstrating and measuring accountability – A discussion Document, Accountability Phase II – The Paris Project, *The Centre for Information Policy Leadership,* p. 2.

[529] Consagrado en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, así como en el artículo 16 (1) del Tratado de Funcionamiento de la Unión Europea (TFUE).

[530]http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part3

[531] Según este autor, "el principio de rendición de cuentas en protección de datos fue introducida como principio separado de la protección de datos en el contexto de las Directrices de la OCDE sobre la protección de la privacidad y los flujos transfronterizos de datos personales**.** Se señalaba por aquel entonces donde no se contemplara la aparición de Internet que el responsable lo era del cumplimiento de medidas y principios como la limitación del tratamiento de datos, la calidad, limitación de los fines de tratamiento, medidas de seguridad, o de principios (menos conocidos) como el de la apertura ("*openness*", párrafo 12) o la participación individual ("*individual participation*", párrafo 13). Lo más determinante lo encontramos en la exposición de motivos de las directrices establece lo siguiente: "El responsable del tratamiento decide sobre los datos y las actividades de tratamiento de datos. Es para su beneficio que se lleva a cabo el tratamiento de los datos. Por consiguiente, es esencial que, con arreglo a la legislación nacional, la responsabilidad del cumplimiento de las normas y decisiones de protección de la intimidad

También el GT29 profundizó en la importancia de la *accountability* demostrando la insuficiencia de *medidas prácticas concretas* en un *dictamen*[532] en el 2010. Y ahora el legislador en la nueva normativa extendió la reflexión del grupo de trabajo y le dio cierta (aunque no lo suficiente) importancia y presencia jurídica que no se había conseguido con la directiva anterior, en particular, con el art. 5.2. RGPD[533], por ejemplo[534].

Pero, *¿cuál es la realidad? ¿qué diferencia existe entre ambas figuras?* Como veremos a continuación, el legislador comunitario perdió una gran oportunidad para aprovechar puesto que permanece sin cambios o dicho con otras palabras, incorporar o clarificar el rol de ambas figuras en el contexto de la economía digital y mercado común (uno de los motivos principales del cambio legislativo), y en particular, en el sector de servicios tecnológicos como cloud computing o IoT:

	Antigua Directiva Europea	**Reglamento Europeo**
Responsable *("controller")*	«responsable del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario (ART. 2.d)	«responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros (art. 4.7).
Encargado *("processor")*	«encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, *solo o conjuntamente con otros,* trate datos personales por cuenta del responsable del tratamiento	«encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento (art. 4.8).

Tabla 21. Cuadro comparativo entre Directiva y Reglamento

---

recaiga en el responsable del tratamiento, *que no debe quedar exento de esta obligación* por el mero hecho de que el tratamiento de los datos sea realizado en su nombre por otra parte, por ejemplo, una empresa de servicios".

[532]Ver Dictamen 03/2010 sobre el principio de responsabilidad. En línea: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_es.pdf

[533] Señala: "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')".

[534] El GT29 decir que la protección de datos tenía que pasar "de la teoría a la práctica" por medio de mecanismos adicionales a los que habían. Con la llegada del RGPD, el legislador parece acercarse a fomentar y dar ciertas responsabilidades al proveedor respecto a la antigua directiva, pero no aún no tiene la amplitud necesaria. Se podría decir que los proveedores tecnológicos, en términos generales, han sido sometidos a un menor grado (aunque también) de rendición de cuentas, mientras que clientes cloud se les obliga a garantizar y demostrar el cumplimiento y eficacia de medidas.

Somos conscientes de que no será nada fácil desdeñar el rol jurídico de los proveedores tecnológicos y sus clientes. La realidad es que los proveedores tienden a escaparse de toda calificación como *responsable* aunque sean los que tengan el control efectivo alegando a lo que señalaba, años atrás, el Dictamen 1/2010[535] sobre los conceptos de responsable ("*controller*") y encargado ("*processor*"). Es decir, una entidad que no tiene ni la influencia jurídica ni fáctica para determinar por qué y cómo los datos personales son procesados no se puede considerar como responsable. El responsable debe tener un control efectivo o autonomía sobre las operaciones de procesamiento -qué y cómo de una operación-, como de las medios esenciales y de las cuestiones técnicas y prácticas -qué software o hardware se utilizará-.

El GT29 (2010, 25) se reafirma al establecer que "un encargado que va más allá de su mandato y adquiere un papel relevante en la determinación de la fines o los medios esenciales de procesamiento es un responsable (o *"joint controller")* en lugar de un encargado".

Los datos personales de salud son de categoría especial por lo que requerirán de una especial atención.

El objetivo de este punto será determinar la rendición de cuentas del cliente *cloud/IoT* y del proveedor *cloud/IoT* en un escenario donde estos últimos son los generadores de grandes riesgos en sus tecnologías correspondientes.

2.1.1. En cloud computing[536].

Esta oscuridad jurídica se extendía también a la interpretación de las figuras jurídicas de los servicios de cloud y sus complejas relaciones. Antes del nuevo Reglamento europeo debido a la definición demasiado "simplista" que proporcionaba el regulador no se podía distinguir claramente la figura del cliente cloud y la del proveedor cloud[537]. Converso (2013) tiene algunas ideas a señalar respecto a la rendición de cuentas, protección de datos y las obligaciones de responsable y encargado como son:

[535] *Supra Cit.*
[536] Pérez Campillo, L. (2017). Novedades del nuevo GDPR en cloud computing. *ITUsers.* Recuperado de https://blogs.itdmgroup.es/lorena-p-campillo/2017/04/novedades-del-nuevo-gdpr-en-cloud-computing-mas-sombras-que-luces
[537] Van Alsenoy (2012). Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC, *Computer Law & Security Review,* p.

i. Inspirarse en la Ley de Protección de Datos Canadiense donde interpretamos que el responsable cloud será el que tenga información personal en su custodia[538].

ii. Inspirarse en la Directiva Europea de Comercio Electrónico donde interpretamos que el proveedor de servicios de cloud computing es un "proveedor de servicio de Sociedad de la Información"[539].

Para el autor estas medidas permitirían de alguna manera igualar o equilibrar las obligaciones de estas figura en relación con la rendición de cuentas. Actualmente con la nueva normativa, continúa el debate acerca de la figura jurídica que ocupan los proveedores y clientes de los servicios cloud. En términos generales y a mi modo de ver, podemos decir que los proveedores cloud definen los elementos esenciales de los *medios*[540] con los que se están tratando los datos, los períodos de retención de datos, las empresas subproveedores que pueden acceder a los datos, etc. En cambio, el cliente de los servicios cloud, en principio, define qué datos se pone a disposición en el entorno de la nube. Por tanto, en ese sentido, desde un punto de vista etimológico y con el Reglamento europeo actual en la mano, se le podría considerar más "co-responsable" que "encargado" del tratamiento de datos en cloud.

Ahora bien, nos encontramos ante una situación paradójica. Aunque etimológicamente se podría hacer ese encuadramiento, los encargados no entrarían en el marco de responsables ya que, *por regla general*, no persiguen sus propios fines. Y por

40 en Converso, D.; "The accountability of data controllers in relation to Cloud providers". Tilburg University, Julio 2013. Recuperado de http://arno.uvt.nl/show.cgi?fid=131417

538 Minister of Justice Canadá (2000). Personal Information Protection and Electronic Documents Act. Recuperado de http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf (ultima modificación 2019). (El cuarto principio señala : "Las organizaciones deben implementar políticas y prácticas para dar efecto a los principios, incluyendo (a) implementar procedimientos para proteger la información personal; (b) establecer procedimientos para recibir y responder a quejas y consultas; (c) capacitar al personal y comunicarle información sobre las políticas y prácticas de la organización; y (d) desarrollar información para explicar las políticas y procedimientos de la organización).

539 No obstante, como señala el autor, ésta "no se aplica expresamente a las cuestiones relativas a los servicios de sociedad de la información cubiertos por la normativa europea de protección de datos (Directiva en aquel momento)". La Directiva, en su artículo 2 (b)contiene el papel del "Proveedor de Servicios", definiéndola como "cualquier persona física o jurídica proporcionando un servicio a la sociedad de la información".

540 También se puede decir que determinar los propósitos y los medios equivale a determinar respectivamente el "por qué" y el "cómo" de determinadas actividades de transformación.

otro lado, los clientes *cloud* podrían omitir su condición de responsable porque, *en ocasiones*[541], no determinan los medios esenciales como son el objeto, la duración, etc. Por tanto, no todo es negativo. Como hemos venido diciendo en los capítulos anteriores, en el RGPD parece arrojarse luz a este dilema jurídico con la previsión de la figura del "corresponsable" (art. 26) en tanto que se pueda delimitar y despejar esa controversia conceptual entre ambas figuras[542][543].

2.1.2. En Internet de las Cosas

Como decíamos, "la aplicación de IoT implica casualmente la intervención combinada de múltiples partes interesadas, como fabricantes de dispositivos, plataformas sociales, aplicaciones de terceros, prestamistas o arrendatarios de dispositivos, corredores de datos o plataformas de datos" (GT29, Dictamen 8/2014). El complejo entramado de las partes interesadas exige la necesidad de una asignación precisa de responsabilidades entre ellas en relación con el tratamiento de los datos personales en función de sus operaciones. Recordemos lo siguiente:

En primer lugar, los fabricantes de dispositivos como Apple, FIT bit o Samsung decidirán la finalidad del tratamiento (y en caso de que exista mas de uno tendrá su correspondiente legitimación, por ejemplo, con su correspondiente consentimiento) y elementos esenciales de los medios, es decir, del porqué y el cómo. Tendrán la obligación de rendir cuentas informando del tratamiento de datos (Art. 13 y 14 RGPD) acerca del tipo de datos que son recogidos por los sensores y los que se tratarán después y cómo. Los fabricantes como responsables deberán rendir cuentas, frente a los titulares de datos respecto al tipo, frecuencia y tiempo de la recogida y almacenamiento de datos personales de salud por sensores

[541] Pensemos en las situaciones donde los clientes de cloud coinciden con los titulares de datos personales y son usuarios finales. Me refiero a aquellos casos en los que las personas físicas son clientes de servicios de almacenamiento de proveedores como Dropbox, por ejemplo, y los medios están prefijados por contratos de formato clickwrap o similar.

[542] Señala que "1.Cuando dos o más responsables determinen *conjuntamente* los *objetivos y los medios* del tratamiento serán considerados *corresponsables del tratamiento*. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos. Dicho acuerdo podrá designar un punto de contacto para los interesados."

[543] De ese precepto se puede extraer varias ideas como que entre ambos pueden; (i) determinar el objetivo (almacenamiento de determinados datos de personas, datos de seguimiento de salud) y los medios (software, apis, duración, etc.); (ii) determinar sus responsabilidades de forma transparente en caso de incumplimiento de RGPD frente a los interesados; (iii) determinar obligaciones frente a los titulares (ej. derechos acceso, portabilidad, oposición a tratamiento automatizado, etc.) y obligaciones de información sobre el tratamiento; (iii) designar un contacto en común para los interesados.

como podómetros[544]. A mi modo de ver, el GT29[545] señala la mejor herramienta de rendición de cuentas posible sería una *opción hipotética* (que permitiera al titular seleccionarla y comunicar con ella la oposición a la recogida,la cual funcionaría como un botón de activación de wifi o opción avión donde se podría dar permiso a facilitar nuestros datos o no. Sería similar a la de un Smartphone como este:

Imagen 61. Ejemplo "botón" de off de transmisión de datos personales. Fuente: Support.apple.

En segundo lugar, los desarrolladores de API crearán aplicaciones móviles[546] que permitirán desarrollar un acceso a los datos a través de dicha API. Por ello, salvo que sea información anonimizada (medida que debería aplicarse tratándose de datos de categoría especial), el desarrollador en el momento en el que tiene acceso a esos datos, se convierte en responsable del tratamiento. Como responsable deberá cumplir el deber de información (art. 13 y 14 RGPD en caso de que no le hayan dado facilitado la información los propios interesados) de una forma continua a través de avisos o notificaciones.

En tercer lugar, se encuentran organizaciones de la industria del cuidado de la e-Health o instituciones de *empresas aseguradoras* que deberán rendir cuenta, sean encargados o responsables, a los usuarios y titulares de datos personales. Por ejemplo, *laboratorios farmacéuticos* como responsables del tratamiento pueden encargar a desarrolladores que diseñen una API para crear una apps (como Social Diabetes) y que tendrán obligaciones de encargado de tratamiento. A su vez, el desarrollador de API, podrá subcontratar a otros desarrolladores o proveedores como redes sociales. Por su parte, las

[544] Así, cuando tenga rol de encargado, es decir, haga el tratamiento siguiendo las indicaciones del responsable o actuando por cuenta de éste (por "delegación"), deberá ser capaz de desarrollar un sistema o método que permita "hacer llegar" a los demás intervinientes (subproveedores, desarrolladores, etc.) que un interesa retira su consentimiento o se opone). O también, proporcionarán herramientas fáciles para notificar vulnerabilidades de seguridad. En definitiva, tengan rol de responsables o encargados deberán rendir cuentas respecto a los principios de protección de datos personales y del RGPD; principio de minimización, transparencia, privacidad desde el diseño, etc.

[545] Según el grupo de trabajo, "para evitar el seguimiento de localización, los fabricantes de dispositivos deben limitar la huella dactilar del dispositivo mediante la desactivación de las interfaces inalámbricas cuando no se utilicen o deban utilizar identificadores aleatorios (como direcciones MAC aleatorias para escanear redes wifi) para evitar un identificador persistente de sea utilizado para el seguimiento de la ubicación.

[546] Dichas aplicaciones se instalan tradicionalmente en base al opt-in donde en puede que esté sometido al consentimiento pero no siempre en las solicitudes está contenida suficiente información para considerar al consentimiento como específico y suficiente. Por ejemplo, la aplicación *Social Diabetes*, contempla en su política de privacidad que los datos son disociados, agregados y anónimos y respecto a las finalidades, mencionar que una de ellas era promocionar productos o servicios de Social Diabetes o de terceros entre los titulares, o invitarles a participar en los cuestionarios, encuestas, y estudios de Investigación para contribuir a la investigación. No obstante, a mi parecer faltaría más información específica a incluir (art. 13 y 14 RGPD).

plataformas de datos con múltiples participantes como *Salus+coop*[547] o *my data*[548] donde intervengan IoT deberán rendir cuentas a los titulares de datos de salud sobre las cuestiones mencionadas anteriormente, sean responsables o encargados.

Responsables IoT	Encargados IoT
Fabricantes de dispositivos (si deciden utilidad y medios): el porqué y el cómo.	Fabricantes de dispositivos (si siguen instrucciones de responsables)
Desarrolladores API (transforman los datos al acceder)	Desarrolladores API (si siguen instrucciones de responsables)
Ind. Farmacéutica y aseguradoras salud (si deciden utilidad y medios): el porqué y el cómo.	Ind. Farmacéutica y aseguradoras salud (si siguen instrucciones de responsables).
Plataformas de datos (si deciden utilidad y medios): el porqué y el cómo. Ej. Una red de investigación formada por hospitales, clínicas, médicos y pacientes de eHealth.	Plataformas de datos(si siguen instrucciones de responsables)

Tabla 22. Cuadro comparativo entre responsables y encargados IoT.

2.1.3. En Blockchain

¿Accountability o liability? Como decíamos la *rendición de cuentas* suponía un reconocimiento demostrable de que los participantes en redes de blockchain/DLT asumen responsabilidad mediante políticas y buenas prácticas, se toman decisiones responsables y en caso de incumplimiento, pueden recibir sanciones. Por tanto, y desde mi humilde punto de vista, convendría más referirse a la responsabilidad con el término más amplio "accountability" o responsabilidad proactiva del responsable del art. 5.2. RGPD [549] que con el concepto de responsabilidad del art. 82 RGPD [550]. Por su parte, la *responsabilidad proactiva* (o *rendición de cuentas)*, "va más allá de la o "liability"[551] o responsabilidad, como algunos autores se han podido referir (Giannopoulou , 2018) [552]

[547] RRI Tools (28 febrero 2019). Salus.coop, un marco para un enfoque dirigido por los ciudadanos a la gestión y gobernanza colaborativa de los datos de salud. Recuperado de https://www.rri-tools.eu/-/salus-coop-a-framework-for-a-citizen-led-approach-to-the-collaborative-managing-amp-governance-of-health-data

[548] Vid. http://www.myhealthmydata.eu/tag/ehealth/

[549] "El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

[550] "Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos".

[551] En esta línea, *Giannopoulou* señalaba que " la responsabilidad ("liability") de los agentes en el almacenamiento o tratamiento de datos a través de una blockchain depende, en primer lugar, de la cualificación de los datos almacenados en cadenas de bloques como datos personales". Este autor se pregunta la clave de la cuestión: ¿qué agentes en el contexto de blockchain serán susceptibles de ser calificados como responsables y encargados del tratamiento de datos según el RGPD?

[552] *Supra Cit.*

[553], porque no se limita a designar quién es responsable de una acción, sino que también exige que la entidad que lleve a cabo la tarea pueda rendir cuentas, dar una razón o una explicación para justificar esa acción. Mientras que en *cloud computing*, la delimitación de roles es más sencilla (el cliente cloud es el responsable y el proveedor cloud es el encargado) en blockchain resulta más complicado ya que no es fácil determinar cómo los participantes usan la tecnología (o impactan sus actuaciones) en el almacenamiento o el tratamiento de datos.

Lo que es claro que la responsabilidad potencial y rendición de cuentas variará en función del diseño y tipo de blockchain y además, su naturaleza propia obliga que todas las redes compartan y validen el libro mayor de información. Esto se traduce en que no solo hay un encargado de datos, y de hecho, se podrían aplicar este papel a todos los nodos que validan las transacciones[554].

Habiendo terminado de abordar la responsabilidad proactiva de responsables tecnología por tecnología y llegados a este punto me parece interesante señalar unas siglas de gran actualidad en el ámbito tecnológico[555]; "*GRC*"[556] ("*gobernance & risk & compliance*") aplicadas también al ámbito de la protección de datos y privacidad. En los próximos apartados desarrollaremos más cada uno de esos términos en relación a la protección de datos.

---

[553] En este sentido, Giannopoulou señala: "La responsabilidad de los actores por el almacenamiento o procesamiento de datos a través de una red de cadenas de bloques depende, en primer lugar, de la calificación de los datos almacenados en las cadenas de bloques como datos personales".

[554] Pero en el RGPD, el legislador no previó que los nodos individuales o mineros individuales son incapaces de validar por sí solos ya que requieren del consenso y las normas incorporadas. En todo caso, en el marco de la gobernanza se debería identificar qué miembros serían los responsables potenciales del tratamiento de datos y qué miembros solamente participan pasivamente en la red y resultan ser simples encargados de datos potenciales.

[555] Vid. https://www.cio.com/article/3206607/what-is-grc-and-why-do-you-need-it.html

[556] La "GRC" ha evolucionado a partir de la gestión del riesgo como una actividad de cumplimiento de la transacción o para añadir valor empresarial, mejorando la toma de decisiones operativas y de planificación estratégica. A grandes rasgos, se puede decir que el concepto de riesgo *("risk")* se asocia con el de *oportunidad.* Después de detectar un riesgo, viene la oportunidad para mejorar la empresa. Conocer detalladamente los riesgos legales de la empresa permitirá prevenir, detectar y gestionar de forma temprana y conociendo las áreas de negocio. Este será el primer paso para que el departamento jurídico en su actuación proactiva desde la prevención en materia de protección e datos. Por ejemplo, los gestores de riesgos buscan amenazas de la competencia, las situaciones políticas y las nuevas regulaciones como el RGPD y la LOPDGDD que podrían afectar el negocio. Por su parte, el gobierno corporativo ("*gobernance")* hasta los días de Enron[556], estuvo escondido pero en la actualidad está mucho más ligado a la gestión de riesgos y al compliance. El gobierno corporativo se focaliza en el control interno corporativo pero centrando su atención en lo que hay a su alrededor. Piénsese en los proveedores tecnológicos que gestionan datos de clientes, usuarios y/o pacientes. Y por último, nos referiremos al cumplimiento normativo ("c*ompliance*") como la acción de controlar o velar por el cumplimiento de las obligaciones que afectan a la organización o institución en materia de protección de datos.

1.2.El análisis de riesgo.

El riesgo[557] va inherente a cualquier actividad realizada por las personas y los tratamientos de datos personales no se quedan atrás; también son actividades realizadas por personas (y por "máquinas")[558] por ello, requieren de una interpretación del riesgo en un par sentidos. En primer lugar, el tratamiento de datos implica un riesgo para la propia organización o institución que lleva a cabo el tratamiento y una gestión del riesgo no apropiada podría suponer repercusiones nada positivas sobre la organización responsable como daños reputacionales corporativos, responsabilidad civil frente a perjudicados, pérdida de negocio y de ingresos, etc. En segundo lugar, los tratamientos de datos que no estén en sintonía con una adecuada gestión de riesgos podrían acarrerar "consecuencias directas negativas" para los titulares de datos como por ejemplo, dificultades para acceder a un puesto de trabajo, discriminación social, etc. Además, en el caso de los datos de salud el riesgo aumenta y su repercusión en las personas cuyos datos pudieran verse afectados negativamente podrían variar en función del tipo de dato de salud y del titular. Piénsese en casos reales o potenciales como :

i. *La brecha de seguridad en el sistema de alojamiento cloud* de un laboratorio (como el laboratorio francés *Labio*) o cualquier hospital[559] donde sus historiales clínicos asociados a pacientes identificables han sido extraídos y vendidos en el mercado negro. El laboratorio u hospital en cuestión será víctima de ciberdelitos como la ciberextorsión (Art. 243 CP)[560][561] con el perjuicio económico que puede

[557] Adelantamos que con carácter general el análisis y la gestión de riesgos en el RGPD, se encuentran estrechamente relacionados con el cumplimiento de lo previsto en los artículos 32 y 35 del RGPD: Artículo 32.1: "Teniendo en cuenta *el estado de la técnica*, los *costes de aplicación*, y la *naturaleza,* el *alcance,* el c*ontexto* y los *fines* del tratamiento, así como *riesgos* de probabilidad y *gravedad* variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar *un nivel de seguridad adecuado al riesgo*, …" · Artículo 35.1: "Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, *entrañe un alto riesgo* para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales…".

[558]Piénsese en las decisiones individuales automatizadas, incluida la elaboración de perfiles (Art. 22 RGPD)

[559] Vid. https://cuadernosdeseguridad.com/2018/04/alertan-del-incremento-de-ciberataques-a-equipos-medicos-en-2018/

[560] "El que, con ánimo de lucro, obligare a otro, con violencia o intimidación, a realizar u omitir un acto o negocio jurídico en perjuicio de su patrimonio o del de un tercero, será castigado con la pena de prisión de uno a cinco años, sin perjuicio de las que pudieran imponerse por los actos de violencia física realizados".

[561]Vid. https://www.technologyreview.es/s/5591/el-hospital-secuestrado-por-un-ciberataque-ha-pagado-el-rescate-de-15000-euros

suponer si acepta el pago del secuestro además de la repercusión pública y desprestigio que le acompañarán. Los pacientes en función del tipo de información y la sensibilidad médica de su historial clínico y enfermedades podrían sufrir de aislamiento social, de discriminación social o laboral y de discriminación frente a sectores como el de las aseguradoras o de las financieras.

ii. El *hackeo de datos personales de salud extraídos de un dispositivo IoT* de juguetes sexuales (como *We-vibe*)[562].Por un lado, la empresa de dispositivos tendrá que indemnizar a los perjudicados y la repercusión pública que tendrá la noticia castigará notablemente a su reputación corporativa. Y por el otro, los usuarios y titulares de datos personales han perdido el control de su información personal e íntima en un ámbito muy privado, información como la frecuencia de las relaciones sexuales o la temperatura corporal.

iii. La *exposición hipotética de datos de salud* de carácter oncológico asociado a una persona identificable publicados en una plataforma e-Health de pacientes (como *Patients like me*) que resulta ser indexado por un motor de búsqueda y recogido a su vez por una aseguradora o financiera para la medición de primas de seguro o la concesión de un préstamo. Plataformas con ánimo de lucro pueden poner en juego su reputación corporativa perdiendo colaboraciones de las más importantes organizaciones farmacéuticas del mundo ante posibles escándalos de brechas de seguridad. Por su parte, los pacientes sufrirán parecidas consecuencias que en el caso anterior. [563]

A priori, el enfoque de riesgos del RGPD se traducirá en dar respuesta a las *medidas necesarias* para garantizar la seguridad de los datos personales y a la necesidad de evaluar con carácter previo el impacto que un tratamiento de datos pueda tener para los derechos y libertades de las personas físicas (ver art. 32 y 35). Entre los posibles riesgos para las personas físicas a los que se refiere el RGPD se encuentran los mencionados en el considerando 75 (algunos coincide con los expuestos en párrafos anteriores): "daños y perjuicios físicos, discriminación, usurpación de identidad, pérdida

[562]Vid. https://www.eldiario.es/theguardian/fabricante-vibradores-indemnizar-clientes-espiarles_0_622238697.html

[563] Con todo ello, se plantea la necesidad de hacer uso de metodologías de *análisis y gestión del riesgo* que ayuden a los responsables (en su mayoría, clientes de servicios tecnológicos) y a encargados del tratamiento (en su mayoría, proveedores tecnológicos) a mantener en continua revisión los riesgos existentes dentro de su organización. El éxito de estas metodologías se manifestarán en la eliminación de riesgos tanto para la organización o institución que realiza el tratamiento como para las personas físicas cuyos datos están siendo tratados de alguna manera (ver. Art. 4.2. RGPD).

de reputación, daños a la confidencialidad y, perjuicios sociales". El RGPD determina dos *niveles de riesgos* con relación a los tratamientos de datos personales: tratamientos de *alto* riesgo y de *escaso* riesgo[564].

En función de estos *niveles de riesgo* se plantea la necesidad de llevar a cabo análisis de riesgos y evaluaciones de impacto. En el caso de tratamientos de escaso riesgo para los derechos y libertades de las personas, sería posible abordar el tratamiento de datos personales únicamente con la implantación de las medidas mínimas necesarias para garantizar la seguridad de los datos. En otros casos, como los que estamos estudiando, con datos de salud relativos usuarios y/o pacientes sería necesario llevar a cabo un *análisis de riesgos* para implantar las medidas técnicas y organizativas pero también sería necesaria la *realización de una evaluación de impacto (EIPD)* cuando se pretenda realizar un cambio sobre un tratamiento de alto riesgo ya existente o cuando se esté diseñando un tratamiento de datos de alto riesgo (protección de datos desde el diseño).

En esta línea y siguiendo *la Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD* de la AEPD (2018) [565], los pasos a tener en cuenta podrían ser:

---

[564] *Centre for Information Policy Leadership* , CIPL (21 de diciembre de 2016). *Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR.* Recuperado de https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf . (Ya señaló que no era clara la definición del "riesgo" en Europa. El mayor problema está en diferenciar los conceptos de "riesgo" y el "alto riesgo", y ésta resultaría muy útil para permitir a las organizaciones y a los reguladores a "priorizar". A mi modo de ver, en efecto, el legislador en el RGPD podría haber previsto una definición del riesgo en función del grado y probabilidad, ya que no es del todo clara la definición).

[565] AEPD (2017) Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD. Recuperado de https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf

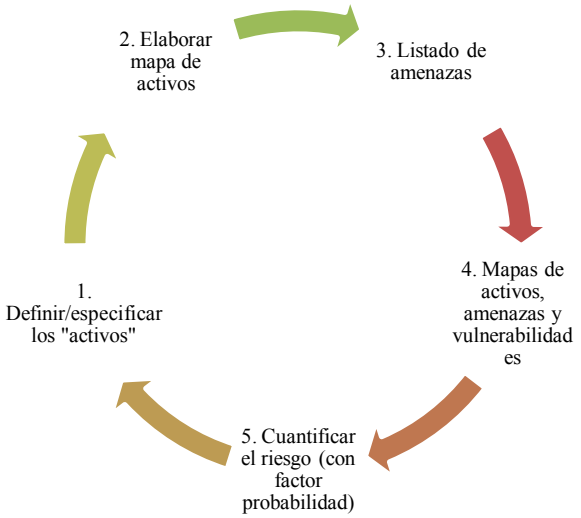


Tabla 23. Pasos a seguir en el análisis de gestión de riesgos según la AEPD.

1. Definir con exactitud aquello que se quiere proteger ("activos").
2. Elaborar un mapa de activos donde incluir todos los medios necesarios para llevar a cabo los objetivos de una organización[566].
3. Elaborar una relación de posibles "amenazas" definiendo las medidas que se tomarían para evitar el impacto de las mismas sobre los derechos y libertades de las personas. A continuación, señalamos ejemplos de riesgos y medidas que ha incluido la AEPD en su guía:

Tipología de riesgo	Riesgo	Medidas de control
Integridad de los datos personales	Modificación o alteración de datos personales no intencionada	▪ Segregación de funciones mediante perfiles de acceso ▪ Controles de monitorización de amenazas en red
Disponibilidad de los datos personales	Pérdida o borrado no intencionado de datos personales	▪ Copias de seguridad ▪ Almacenamiento en dos ubicaciones diferentes
Confidencialidad de los datos personales	Acceso no autorizado a los datos personales	▪ Mecanismos de control de acceso ▪ Segmentación de la red
Garantizar el ejercicio de los derechos de los interesados	Ausencia de procedimientos para el ejercicio de derechos	▪ Procedimientos y canales para el ejercicio de derechos
Garantizar los principios relativos al tratamiento	Ausencia de legitimidad para el tratamiento de los datos personales	▪ Cláusulas informativas y base legitimadora para el tratamiento de datos
	Tratamiento ilícito de datos personales	▪ Monitorización del uso de datos personales

[566] Por ejemplo, para un hospital y su departamento de investigación, una empresa de dispositivos IoT eHealth, una aseguradora e-Health, una organización de la industria farmacéutica puedan desempeñar sus funciones sin ocasionar perjuicios a los derechos de los usuarios, pacientes o titulares será necesario disponer de fluido eléctrico permanente, sistemas de información para la gestión de historiales clínicos para almacenar y gestionar la base de datos de de los usuarios, pacientes o titulares, y equipos informáticos para las funciones o mecanismos que garanticen los derechos de los interesados. Por su parte el registro de actividades (ver art. 30 RGPD y guía) de tratamiento puede ser un recurso de base para la puesta en marcha de los análisis de riesgos.

Tabla 24. Tipología de riesgos y medidas de control. Fuente: AEPD

No olvidemos lo que el análisis de riesgos parte de la base de la descripción de las operaciones de actividades de tratamiento *teniendo en cuenta el ciclo de vida* de los datos que podría definirse al menos:

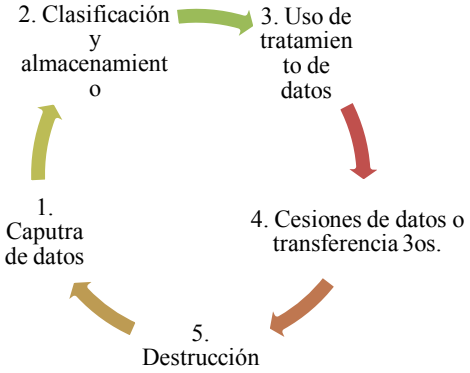


Tabla 25. Análisis de riesgos y ciclo de vida de los datos. Fuente: AEPD

4. Tener en cuenta los mapas de activos, de amenazas, y de vulnerabilidades específicos para cada tratamiento. Desde un punto de vista práctico, el análisis de riesgo proporciona una visión general a los responsables y encargados del tratamiento que habitualmente suele representarse mediante *mapas de calor* que llevan asociado un valor cuantitativo. Así por ejemplo, la experta Hilary Wandall mostró como la implantación de control de riesgos en el caso de aplicaciones móviles de salud (y el caso de gestión de nóminas, de interés para su comparación) podían hacer disminuir del riesgo alto a bajo.

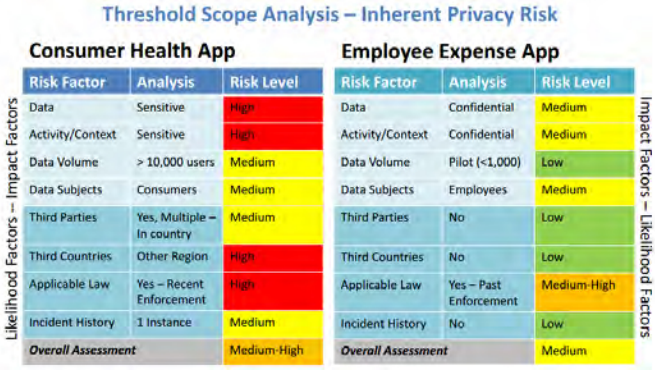


Imagen 62. Ejemplo de riesgos de privacidad en una app de salud y las nóminas de los empleados. Fuente: IPC[567]

5. Asignar un valor cuantitativo[568] o cualitativo teniendo en cuenta el factor de la "probabilidad" de que una amenaza pueda llegar a materializarse. En términos generales el riesgo se mide teniendo en cuenta la probabilidad de que una amenaza se materialice y el impacto que podría suponer para la organización o para los propios interesados, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento y la capacidad de mitigar un "alto riesgo "y el tipo de tecnología. En todo caso:

[567] Vid. https://www.informationpolicycentre.com/
[568] Vid. Malin B. (2017) Quantitative Methods to Measure the Risk of Re-identification: Methodology Review. Recuperado de https://www.ema.europa.eu/en/documents/presentation/presentation-quantitative-methods-measure-risk-re-identification-b-malin_en.pdf

Riesgo= Impacto x probabilidad

Tal como señaló el *CIPL*[569] (2016), "las orientaciones futuras deberían aclarar que los términos de procesamiento *a gran escala, evaluación sistemática y exhaustiva* y *control sistemático* del RGPD requieren que las organizaciones los interpreten caso por caso y en el contexto de sus propias operaciones, reconociendo que las organizaciones deben ser capaces de justificar sus interpretaciones". Por otro lado, y de gran relevancia sería mencionar la particularidad del análisis y gestión de riesgos en la cadena de suministro de los proveedores tecnológicos. En definitiva, el *análisis y la gestión del riesgo* trata de poner *una cifra de referencia* (umbral de riesgo aceptable) sobre el que una organización tiene que marcar sus objetivos de riesgo para, posteriormente, llevar a cabo un proceso de gestión de los mismos y la revisión de la eficacia de las medidas utilizadas (auditoría)[570] para eliminar o atenuar el nivel de riesgo[571]. El planteamiento de las metodologías de análisis de riesgos podría resumirse con carácter general en, al menos, las cuatro fases siguientes:

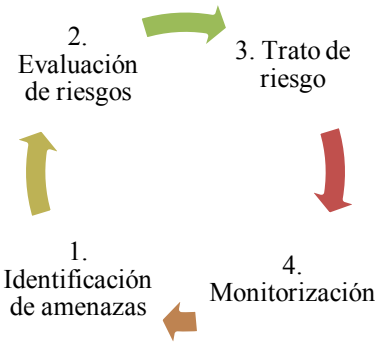


Tabla 26. Fases de las metodologías de análisis de riesgos.

A modo de conclusión, me gustaría destacar el esfuerzo del legislador y regulador en "estandarizar" la gestión de riesgos en materia de protección de datos. Si bien ésta no altera los derechos y obligaciones resulta ser una herramienta valiosa para

[569] *Supra cit.*

[570] Tal y como se señala en la guía, el análisis y la gestión de riesgos "es un proceso consciente, metodológico y estructurado que debe adecuarse en todo momento a la evolución del riesgo, por tanto, es un proceso de *mejora continua* y no puede ser interpretado como un proceso cerrado", "tras la monitorización de los resultados mediante auditorías es necesario realimentar el proceso añadiendo de *nuevas amenazas* que hubieran sido identificadas de las que pudiera tenerse constancia de cualquier fuente de información (registro de incidencias, información de proveedores de productos, servicios de alerta, noticias de prensa, comunicados de fuerzas y cuerpos de seguridad, etc.) con el objetivo de volver a tratar el riesgo". Los responsables y encargados del tratamiento deben de tener en cuenta una *política de riesgos* que sirva para la toma de decisiones sobre las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales a la que se refiere el artículo 32 del RGPD, las medidas de seguridad deben ser el resultado de la gestión del riesgo y nunca un listado cerrado de medidas.

[571] Algunas normas de referencia a tener en cuenta con relación a la gestión y análisis de riesgos son las normas *ISO 31000 y 31010.*

calibrar *la "accountability"*, en particular, priorizando acciones y en general, creando una cultura de GRC y concienciación acerca de la importancia de identificar riesgos y medidas de mitigación adecuadas.

Ahora bien, el camino es largo y aún quedan pendientes tareas como: (i) desarrollar un consenso en el contexto internacional de los impactos negativos y positivos; (ii) construir un modelo de *best practices* y sectoriales para organizaciones e instituciones que traten datos personales de salud herramientas flexibles para la evaluación de riesgos en materia de datos personales; (iii) profundizar más en "cómo" las organizaciones pueden utilizar la herramienta de la gestión de riesgos para gestionar el cumplimiento en protección de datos.

1.3.La evaluación de impacto.

En la guía (AEPD, 12) se señala que para determinar si es necesario llevar a cabo la EIPD o no, se puede seguir una breve metodología de análisis con dos fases:

- "Fase I: Análisis de las listas de tratamientos previstos en la regulación (art 35.3, 35.4, y 35.5)". "Es importante destacar que, si el tratamiento no está incluido en los supuestos comentados y en ninguna de las listas, no implica que no sea necesario llevar a cabo la EIPD, y en todo caso, será necesario pasar a la segunda fase de análisis".
- "Fase II: Análisis de la naturaleza, alcance, contexto y fines de tratamiento (art 35.1). Esta fase se centra en evaluar las características de las actividades de tratamiento a realizar según los aspectos previstos en el artículo 35.1 del RGPD":
  - *Naturaleza del tratamiento.* Por ejemplo: ¿Se tratan categorías especiales de datos?(sí, en nuestro caso de estudio, puesto que son de salud) ¿Se tratan datos a gran escala? (Sí, piénsese, en analítica de datos en investigaciones) ¿Se hace un seguimiento exhaustivo de las personas? (sí, piénsese, en las investigaciones con pacientes identificables e identificados) ¿Se combinan diferentes conjuntos de datos? (sí, por ej. en investigación, habrán fuentes de información diferentes,) ¿Los datos se refieren a personas en situación de vulnerabilidad? (sí, por ej. en investigación suelen tratarse de individuos con enfermedades diagnosticadas)
  - *Alcance del tratamiento.* Se deben valorar los efectos o consecuencias del tratamiento, identificando hasta qué punto puede llegar y si éste puede suponer un alto riesgo. Por ejemplo: ¿Se realiza un proceso de toma de decisiones con efectos jurídicos?
  - *Contexto del tratamiento.* Por ejemplo: ¿Se realiza un uso de nuevas tecnológicas? (se entiende que la respuesta será afirmativa en todas los análisis de nuestro estudio) ¿son especialmente invasivas para la privacidad? (dependerá el tipo de tecnología) ¿Existen varios responsables del tratamiento? (en el caso de IoT y Blockchain sí, incluso se podría dar en cloud) ¿Existen cadenas complejas de encargados de tratamiento? (sí, suelen darse subcontrataciones) ¿Se producen

transferencias internacionales? (será bastante frecuente salvo que cliente y proveedor se encuentren en territorio europeo, por ej.) ¿Existen cesiones de datos? (también será frecuente).

- *Finalidades del tratamiento.* Se deben identificar cada una de las finalidades del tratamiento y analizar si estas derivan en un alto riesgo. Por ejemplo, si la finalidad incluye: Toma de decisiones, elaboración de perfiles, análisis predictivo, prestación de servicios relacionados con la salud, seguimiento, control y observación de personas (monitorización)". Por ejemplo, pensemos en la monitorización que puede realizar un dispositivo IoT (por ej. FIT bit).

Adicionalmente, con el objetivo de poder determinar qué tipo de tratamientos pueden considerarse de *alto riesgo,* el GT29 en el documento Directrices sobre las Evaluaciones de Impacto en la Protección de Datos (WP248)[572] introduce criterios que pueden evidenciar un elevado riesgo inherente a las actividades de tratamiento y que, se deben evaluar y pueden determinar la necesidad de realizar un EIPD:

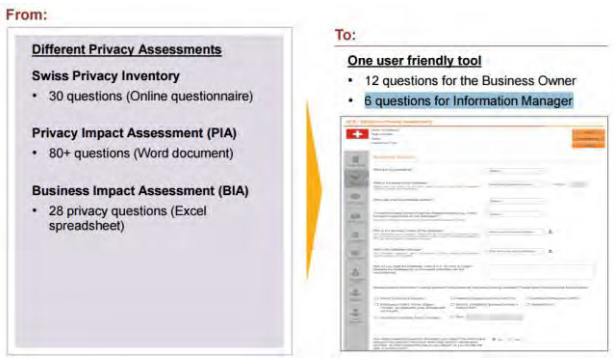
Tipo de tratamiento	DESCRIPCIÓN
Evaluación o scoring	Valoraciones y análisis, incluidos la elaboración de perfiles y predicciones, especialmente de "aspectos relacionados con el desempeño del interesado en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, ubicación o movimientos".
Toma de decisiones automatizada con efecto legal o similar	Procesamiento que tiene como objetivo la toma de decisiones sobre sujetos que producen "efectos legales sobre la persona física" o que "de manera similar afecta significativamente a la persona física". Por ejemplo, si el procesamiento puede conducir a la exclusión o discriminación de las personas.
Monitorización sistemática	Procesamiento utilizado para observar o controlar a los interesados, incluidos los datos recopilados a través de redes o un sistema de control de un área de acceso público[2].
Datos confidenciales o de naturaleza altamente personal	Actividades de tratamiento con categorías especiales de datos personales, por ejemplo, información sobre las opiniones políticas de los individuos o registros médicos, así como datos personales relacionados con condenas penales o delitos.
Coincidencia o combinación de conjuntos de datos	Actividades de tratamiento que implican la combinación de conjuntos de datos. Por ejemplo, procedentes de dos o más actividades de tratamiento de datos realizadas para diferentes propósitos y/o por diferentes responsables del tratamiento de una manera que exceda las expectativas razonables del sujeto de datos.
Datos relativos a las personas vulnerables	Los sujetos de datos vulnerables pueden incluir menores, segmentos más vulnerables de la población que requieren protección especial (personas con enfermedades mentales, solicitantes de asilo o ancianos, pacientes, etc.).
Uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas	Actividades de tratamiento realizadas mediante el uso de tecnología innovadora que pueda implicar nuevas formas de recopilación y uso de datos, posiblemente con un alto riesgo para los derechos y las libertades de las personas. Por ejemplo, la combinación del uso de la huella dactilar y el reconocimiento facial para mejorar el control del acceso físico, etc.
Cuando el procesamiento en sí mismo "impide que los interesados ejerzan un derecho o utilicen un servicio o un contrato"	Operaciones de procesamiento que tienen como objetivo permitir, modificar o rechazar el acceso de los interesados a un servicio o la entrada en un contrato.
Tratamientos sujetos a un código de conducta que lo requiere	Si a los tratamientos evaluados se les aplica un código de conducta que exige su cumplimiento también debe ser objeto de la evaluación.

Tabla 27. Tabla de tipo de tratamientos y riesgos. Fuente: AEPD.

A efectos prácticos, no obstante, deberíamos tener en cuenta algunos aspectos:

[572] GT29. Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679. (WP 248). Recuperado de https://www.aepd.es/media/criterios/wp248rev01-es.pdf

Por un lado, el GT29 señala que el responsable del tratamiento puede considerar que, por *la naturaleza del tratamiento*, aunque los tratamientos cumplen varios de los criterios mencionados, realmente no haya un probable alto riesgo. En este caso, hay que documentar y argumentar de forma clara las razones por las que no se lleva a cabo la EIPD[573].Y es que la regulación no se cierne exclusivamente a una lista de tratamientos concreta a la que se limite la necesidad de realizar una EIPD. En aquellos casos en los que no esté claro, *es recomendable la realización* de la misma. Por otro lado, para que sea efectivo el control de riesgos en la práctica, se requieren de herramientas eficaces, escalables y flexibles[574] [575] de manera que trabajen para las grandes organizaciones (y pymes, también). El siguiente ejemplo expuesto por la experta en privacidad de Novartis en Suiza, *Maria Chiara Atzori*[576], puede dar a entender como el ahorro burocrático y administrativo se traduce en un proceso de gestión de riesgos más efectivo, (pasando de una EIPD de 138 preguntas inconsistentes a 18 preguntas simples y consistentes):



[573] En la Guía se señala que " en el otro extremo, para aquellos tratamientos para los cuales no es necesario realizar una EIPD, el GT 29 establece también ciertos supuestos. Así lo considera, por ejemplo, cuando la naturaleza, el alcance, el contexto y las finalidades del tratamiento son muy similares a las de un tratamiento para el que ya se ha hecho una evaluación, o cuando el tratamiento tiene como base jurídica el derecho del Espacio Económico Europeo o del Estado miembro y la EIPD ya se ha hecho en este contexto. En ambos casos se debe argumentar que efectivamente, nos encontramos ante un tratamiento que encaja claramente en estas circunstancias y por tanto no es necesario llevar a cabo la evaluación".

[574] Este es un enfoque que se tomó en las negociaciones para la elaboración del nuevo reglamento europeo. El Consejo en una nota con fecha de 3 de octubre de 2014 manifestó la necesidad de reducir aún más los costes de carga y administrativos y de dirigir el fin a mejores prácticas aprobando códigos de conducta y certificaciones a través de las indicaciones del responsable. Ver Nota 13772/14, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.*

[575] En la exposición de motivos que acompañaban a las revisiones de las directrices de la OCDE, se dejaba claro que la *gestión de riesgo* estaba intrínsecamente conectada con la *proporcionalidad*. La OCDE indicaba que "para ser efectivo el alcance de cualquier evaluación de riesgos de privacidad, debe ser *suficientemente amplia* como para tener en cuenta el alcance de los daños y beneficios, pero, también, debe ser lo *suficientemente simple* como para ser aplicado de manera rutinaria y consistente". Ver OECD, Data-Driven Innovation, 226.

[576] Vid. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/risk_webinar__24_may_2016_.pdf

Imagen 63. Ejemplo de evaluación electrónica de privacidad. Fuente: Information Policy Centre

El GT29 en el contexto de la aplicación de intereses legítimos en virtud del art. 7 de la (antigua) Directiva ya clarificó que el propósito de la Artículo 7 (f) de equilibrio no era tanto evitar cualquier impacto negativo sobre el tema de datos, sino más bien, "evitar *efectos desproporcionados*". Por tanto, si seguimos la línea de intenciones del grupo de trabajo, concluiremos que el análisis y la gestión de riesgos en los tratamientos de datos personales tienen que estar orientados a una *gestión proporcional* que mitigue los impactos negativos de los mismos impidiendo a ser posible el freno a la innovación y el desarrollo de la economía digital.

A continuación comentaremos posibles evaluaciones de impacto en las tecnologías de cloud, IoT y blockchain de una manera muy sintetizada.

a) En Cloud[577]

	Amenazas/Riesgos	*Medidas*
Laboratorio pruebas clínicas. Cliente cloud (responsable)	-Disociación deficiente o reversible que permita la re-identificación de datos de categorías especiales en	-Cifrado y un amplio uso de las técnicas de anonimización y tecnologías que mejoren mejorar la

[577] Pongamos el caso hipotético de que hablábamos al inicio de este punto. Se produce una brecha de seguridad en el sistema de alojamiento *cloud* de un laboratorio de pruebas médicas y los historiales clínicos asociados a pacientes identificables fueron extraídos y vendidos en el mercado negro y además el laboratorio fue víctima de ciberextorsión (Art. 243 CP) con el perjuicio económico que puede suponer si acepta el pago del secuestro además de la repercusión pública y desprestigio que le acompañarán. Los pacientes en función del tipo de información y la sensibilidad médica de su historial clínico y enfermedades podrían sufrir de aislamiento social, de discriminación social o laboral y de discriminación frente a sectores como el de las aseguradoras o de las financieras.[577] Antes de realizar un método de gestión de datos donde hubiera tratamiento de datos personales de salud que implicara un tratamiento de datos (alojamiento) por parte de un "tercero" (proveedor cloud) sin medidas necesarias (anonimización) según RGPD, al aplicarse éstas se podría pasar de un nivel máximo (tipo 16) a un nivel moderado o limitado (tipo 1-2) en sintonía con la política de riesgos establecida en la institución u organización. Gracias a los controles de seguridad habremos obtenido el umbral de riesgo y con medidas como la citada (o incluso, añadiendo también procesos de auditoría, formación de personal, certificaciones, etc.) mejoraríamos el nivel de riesgo. Además el resultado de los análisis debe incluir un informe de medidas de seguridad y ejecutivo disponible para la toma de decisiones de una organización, el cual servirá como prueba documental del principio de responsabilidad proactiva ("accountability") de los clientes -como responsables- y los proveedores cloud -como encargados del tratamiento-del que hemos hablado en el punto anterior. Aunque también será de gran utilidad para la alta dirección a la hora de orientar esfuerzos y recursos económicos con el fin de reducir, eliminar o trasladar los riesgos a un tercero mediante la suscripción de una posible póliza para cubrir posibles daños a las personas físicas, como por ejemplo, a través de "ciber-seguros". (Ver http://www.thiber.org/wp-content/uploads/2016/06/sic120-ciberseguros.pdf y https://obamawhitehouse.archives.gov/files/documents/cyber/ISA%20-%20Cyber-Insurance%20Metrics%20and%20Impact%20on%20Cyber-Security.pdf). Como hemos dicho, hay que tener en cuenta que las medidas y garantías de mitigación de riesgos se deberán aplicar desde el inicio del proceso y a lo largo del ciclo de vida del dato. El RGPD señala que: "las evaluaciones de impacto de protección de datos en consecuencia, deberían tener en cuenta la totalidad de la *gestión del ciclo de vida* de los datos personales de la colección de procesamiento para su eliminación, la descripción detallada de las operaciones de tratamiento previstas, los riesgos a los derechos y libertades de los interesados, las medidas previstas para hacer frente a los riesgos, las salvaguardias, las medidas y mecanismos de seguridad para garantizar el cumplimiento del reglamento".

	procesos de investigación que solo prevén utilizar datos anónimos. -Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos personales. -Accesos no autorizados a datos personales.	privacidad,etc. -Formación apropiada del personal sobre protección de datos. Comunicación auditable y clara de las responsabilidades del personal en relación con el cumplimiento de las políticas de privacidad de la organización así como de las sanciones aparejadas al incumplimiento de las mismas. -Homologación previa y negociación clausulas contractuales: auditorías[578] independientes[579], certificaciones, adhesión a códigos de conducta, clausulas de penalización ante incumplimiento RGPD/LOPDGDD, rechazo de Clicks-Through..etc. - Seguros de responsabilidad civil (ciberseguros). -Medidas técnicas y organizativas: control acceso, etc.
Dropbox. Proveedor cloud (encargado)	- Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos personales. -Impedimentos por parte del importador (subproveedor) para el ejercicio de los procedimientos de supervisión y control pactados. -Gestión deficiente de las subcontrataciones e insuficiente control sobre encargados y subcontratistas y, en particular, dificultades para comprobar o supervisar que el encargado y los subcontratistas cumplen las instrucciones y, especialmente, las medidas de seguridad. - Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación	-Medidas técnicas y organizativas según RGPD (art. 32 y 35) incluidas técnicas de cifrado y anonimización. -*Homologación previa*[580] del subproveedor cloud. clausulas contractuales: auditorías, certificaciones, adhesión a códigos de conducta, clausulas de penalización ante incumplimiento RGPD/LOPDGDD..etc. Utilizar código de conducta del sector Farmaindustria (y big data) para realizar EIPD como encargado de tratamiento. -Establecer el *período máximo* de almacenamiento así como un procedimiento de destrucción de los datos una vez que se haya cumplido el citado período. -Medidas técnicas y organizativas

[578] Bastantes autoridades de control europeas consideran que los clientes necesitan medios técnicos y prácticos para poder investigar accesos no autorizados sospechosos a datos personales. En cuanto a las auditorías posteriores al contrato según el estudio de la Universidad de *Standford*, muchos clientes –en su mayoría financieros- necesitaban saber que contaban con ese derecho de auditoría (al menos una vez al año) o incluso una especie de "cooperación comercial razonable". Sin embargo, muchos proveedores se negaron por razones de seguridad y sobre todo, por costes. Algunos proveedores SaaS llegan ofrecer herramientas a los usuarios para controlar los accesos a los datos de usuario con registros de monitoreo las 24 horas (para ver quién accede, qué cuentas vieron y qué hicieron). Incluso algún proveedor de SaaS, se comprometió a realizar registro con todos los accesos de serie. Esta medida empezó a sustituir a la auditoría .Se puede entender que este tipo de medidas pueden reforzar la *confianza y transparencia* frente a los proveedores. Aunque algunas autoridades de control europeas de protección de datos, siguen creyendo necesaria la auditoría para PaaS e IaaS (incluso una auditoría al data center).

[579] La autoridad de control sueca *"Datainspektion"* ha considerado a estas auditorías independientes como la solución para que los proveedores y sub-proveedores no se eximan de responsabilidad frente a las medidas de seguridad.

[580] Según la Opinión 05/2012 sobre *Cloud Computing* del GT29: "…una precondición para la confianza en las disposiciones sobre servicios en la nube para el responsable del tratamiento (cliente de servicios Cloud) es realizar un *ejercicio de evaluación del riesgo*, incluyendo la *localización de los servidores donde los datos son procesados* y la consideración de los riesgos y beneficios desde el punto de vista de protección de datos (…)" . Como se ha dicho, el cliente es responsable de la elección del proveedor y del servicio, con todas las consecuencias jurídicas que pueden derivarse; debe acceder a la información que la empresa de nube le facilite; y, al fin y al cabo, controlarlo y auditarlo.

	sobre protección de datos personales.	según RGPD (art. 32 y 35) incluidas técnicas de cifrado y anonimización.
Amazon. Subproveedor cloud(subencargado)	Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos personales. Medidas técnicas y organizativas según RGPD (art. 32 y 35) incluidas técnicas de cifrado y anonimización.	

Tabla 28. Tabla de amenazas/riesgos y medidas a tomar en cloud y Healthcare.

b) En Big Data e IA

	Amenazas/Riesgos	*Medidas*
Consorcio Hospital- Univerisidad UPV	-Fallos o errores sistemáticos u ocasionales para recabar el consentimiento expreso al ser ésta la base legítima. - Garantías insuficientes para el uso de datos personales con fines históricos, científicos o estadísticos. Disociación deficiente o reversible que permita la re-identificación de datos de categorías especiales en procesos de investigación que solo prevén utilizar datos anónimos. - Utilizar los datos personales para finalidades no especificadas o incompatibles con las declaradas: Utilización de los metadatos para finalidades no declaradas o incompatibles con las declaradas. Asunción errónea de la existencia de una habilitación legal para el tratamiento o cesión de datos de categorías especiales. -Accesos no autorizados a datos personales. Falta de formación del personal sobre las medidas de seguridad que están obligados a adoptar y sobre las consecuencias que se pueden derivar de no hacerlo.	-Asegurarse de que no existen otras causas de legitimación más adecuadas. Cuando el tratamiento de datos personales se legitime por una relación contractual, ofrecer siempre la posibilidad de consentimiento separado para tratar datos con finalidades que no son necesarias para el cumplimiento o perfeccionamiento de la misma, evitando incluirlas de forma indisoluble en las cláusulas del contrato. - Siempre que sea posible, utilizar datos anónimos o disociados. Utilizar pseudónimos o atribuir códigos de sustitución de los datos identificativos que, aunque no consigan la disociación absoluta de los mismos, sí que pueden contribuir a que la información sobre la identidad de los afectados solo sea accesible a un número reducido de personas. Garantizar que se aplican las medidas de seguridad adecuadas y correspondientes al nivel de seguridad de los datos utilizados. - Formación personal y control de acceso.
Empresa tecnológica analítica (encargado)	- Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos personales. -Impedimentos por parte del importador (subproveedor analítica) para el ejercicio de los procedimientos de supervisión y control pactados. Gestión deficiente de las subcontrataciones e insuficiente control sobre encargados y subcontratistas y, en particular, dificultades para comprobar o supervisar que el encargado y los subcontratistas cumplen las instrucciones y, especialmente, las medidas de seguridad.	-Medidas técnicas y organizativas según RGPD (art. 32 y 35) incluidas técnicas de cifrado y anonimización. -Homologación previa del subproveedor analítica; clausulas contractuales: auditorías, certificaciones, adhesión a códigos de conducta, clausulas de penalización ante incumplimiento RGPD/LOPDGDD..etc. Utilizar como guía el código de conducta del sector Farmaindustria (y big data) para realizar EIPD como encargado de tratamiento. -Medidas técnicas y organizativas según RGPD (art. 32 y 35) incluidas técnicas de cifrado y anonimización.

Tabla 29. Tabla de amenazas/riesgos y medidas a tomar en Big Data y IA en Healthcare.

c) En Internet de las Cosas

	Amenazas/Riesgos	*Medidas*
Fabricante dispositivo IoT (responsable)	-Fallos o errores sistemáticos u ocasionales para recabar el consentimiento expreso al ser ésta la base legítima. Dificultades para garantizar la legitimidad de la recogida y la cesión de datos personales provenientes de terceros. (generales). Obtener un consentimiento dudoso, viciado o inválido para el tratamiento o cesión de datos personales. - Redactar la información en materia de protección de datos en un lenguaje oscuro e impreciso -Dificultar la revocación del consentimiento o la manifestación de la oposición a un tratamiento o cesión. -Pérdida de competitividad del producto o servicio derivada de los daños reputacionales causados por una deficiente gestión de la privacidad. (generales). -Dificultades para conseguir la portabilidad de los datos personales a otros entornos una vez finalizado el contrato.	- Cumplir con lo establecido en el art. 13 y 14 RGPD (deber de información). Evitar condicionar el disfrute de un producto al consentimiento para finalidades diferentes. - Botón "off" donde el usuario y titular de datos controle el cómo y el tiempo de la recogida de los mismos a través de los sensores. - Estandarización de información para posibilitar realizar portabilidad (no vendor-lock in)
Desarrollador IoT (encargado)	-Disociación deficiente o reversible que permita la re-identificación de datos de categorías especiales en procesos de investigación que solo prevén utilizar datos anónimos. -Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas.	
Aseguradora de salud eHealth (responsable 2)	-Fallos o errores sistemáticos u ocasionales para recabar el consentimiento expreso al ser ésta la base legítima. - Utilizar los datos personales para finalidades no especificadas o incompatibles con las declaradas y cesión de datos a terceros como industria farma sin legitimación legal. -Toma de decisiones económicas, sociales, laborales, etc. relevantes sobre las personas (en particular las que pertenecen a colectivos vulnerables), especialmente si pueden ser adversas o discriminatorias, incluyendo diferencias en los precios y costes de servicios y productos -Falta de diligencia (o dificultad para demostrarla) en la elección del encargado de tratamiento.	- Cumplir con lo establecido en el art. 13 y 14 RGPD (deber de información). - Evitar condicionar el disfrute del servicio al consentimiento para finalidades diferentes

Tabla 30. Tabla de amenazas/riesgos y medidas a tomar en IoT en Healthcare.

d) En Blockchain

	Amenazas/Riesgos	Medidas
Consorcio Hospital- Laboratorio farmacéutico Sanofi-Univerisidad UPV-Tecnológica Philips (responsable)	-Dificultad en determinar la responsabilidad del tratamiento y transparencia a los titulares de datos. -Dificultad en principio de minimización (continuo registro en la cadena de bloques) - Conservación limitada en el tiempo -Dificultar o imposibilitar el ejercicio de los *derechos de los interesados:* a. Dcho. acceso. Los responsables desconocen qué datos son almacenado en la cadena ya que sólo manejan la versión cifrada o hash del dato. b. Dcho. rectificación c. Dcho. supresión (olvido) d. Derecho portabilidad. Poder cambiar de red blockchain sin problemas y sin la perdida de datos. Esto tiene implicaciones en los protocolos de consenso de las redes.	-Herramientas de transparencia (5.1.a. RGPD) - Fórmulas cifrado sólido (conocimiento cero) a. Registro fuera de la cadena para los datos transaccionales pero sigue resultando inviable para los datos de las claves públicas. b.Uso de enlaces a datos con la rectificación fuera de la cadena de bloques (Guy Zyskind). c. Teniendo en cuenta el art. 17.2 RGPD: exención técnica a blockchain. Soluciones como la poda , hash de camaleón, offchain, sidechain.
Nodos (Encargados)	-Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas	- Smart contract recogerá las clausulas para los intervinientes en el consorcio.
Desarrollador Smart Contract (Encargado)	-Disociación deficiente o reversible que permita la re-identificación de datos de categorías especiales	-Utilizar código de conducta del sector Farmaindustria (y big data) para realizar EIPD como encargado de tratamiento
BaaS (subencargado)	Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos personales. Solución: Medidas técnicas y organizativas según RGPD (art. 32 y 35) incluidas técnicas de cifrado y anonimización.	

Tabla 31. Tabla de amenazas/riesgos y medidas a tomar en Blockchain en Healthcare.

Un último apunte subrayando algo que hemos citado en párrafos anteriores: la importancia de los ciberseguros. Es tan relevante esta cuestión que incluso el SEPD[581] abre la puerta a la obligatoriedad de los ciberseguros.

1.4.La gobernanza de datos

La gobernanza de los datos según el profesor Javier Puyol[582] "responde fundamentalmente el establecimiento de un programa global e integral para gestionar todos los datos de una empresa, tomando en consideración elementos organizativos, políticos y arquitectónicos de la estructura que se quiere establecer para que dicha gestión sea verdaderamente eficiente". O dicho por otras palabras; "la gobernanza de los

[581] Ponce de León, M. (7 de marzo de 2019). El supervisor europeo abre la puerta a la obligatoriedad de los ciberseguros. Recuperado de http://www.expansion.com/empresas/banca/2019/03/07/5c80277122601d7b6b8b45e8.html

[582] Puyol, J. (20 de noviembre de 2016). ¿Qué es el "Data Governence o gobernanza de los datos"? *Confilegal*. Recuperado de https://confilegal.com/20161120-data-governance/

datos trata de dotar de ventajas competitivas a las empresas, que les permiten mediante el uso de los datos o sentar posiciones de liderazgo en su ámbito de negocio"[583] . El profesor quiere puntualizar, además, que no es lo mismo gobierno de los datos que gestión de los datos; " el gobierno de los datos es el marco de elaboración de políticas y derechos de decisión para los datos corporativos, mientras que la gestión de los datos es la ejecución táctica de dichas políticas". Esta diferencia es importante. Además, resalta la importancia de que "cada día va cobrando más fuerza e importancia comprender y promover la importancia de los *activos de carácter inmaterial*, representados en este caso, por los *datos de carácter personal,* incluso aunque los mismos se encuentren anonimizados, sean estos estructurados o desestructurados" [584] [585].

---

[583] El profesor Puyol, destaca que "Según IBM, el establecimiento de un proceso de "Data Governance" debe estar basado en el cumplimiento de una serie de pautas o criterios que son los que se enuncian a continuación: a). Establecer metas. Sentencias principales que guían la operación y desarrollo de la cadena de suministro de información). Definir métricas. Conjunto de medidas usadas para evaluar la efectividad del programa y los procesos de gobierno asociados). Tomar decisiones. La estructura organizacional y el modelo de cambio ideológico para analizar y crear políticas de decisión). Comunicar políticas. Herramientas, habilidades y técnicas usadas para comunicar decisiones políticas a la organización. e). Medir resultados. Comparar resultados de las políticas con las metas, entradas, modelos de decisión y comunicación para proveer constante retroalimentación sobre la efectividad de la política). Auditar. Herramienta usada para comprobar todo". Vid. Cfr.: IBM. "Seis pasos para el Gobierno de Datos. ¿Qué es y cómo se implementa un programa de gobierno de datos?

[584]Vid. Power Data. *El gobierno de datos eficaz. La guía para minimizar errores y alcanzar objetivos de gobernanza de datos.* Recuperado de https://cdn2.hubspot.net/hubfs/239039/docs/Ebook-Gobierno-Datos-Eficaz.pdf?t=1495399698278 (Un programa de gobierno de datos incluiría, al menos: (i) "Un *órgano de gobierno o consejo*: que se encargará, entre otras funciones, de definir los roles de los propietarios o custodios de los activos de datos en la empresa. Asimismo, deberán desarrollar políticas que ayuden a especificar quién es responsable de cada una de las partes o aspectos de los datos, incluyendo su exactitud, la accesibilidad, la coherencia, la integridad y la actualización. (ii) Un *conjunto definido de procedimientos:* que explique el modo en que los datos se van a guardar, los sistemas de almacén que se emplearán, las medidas de seguridad y protección contra accidentes, robo o ataque aplicables. Por supuesto, conviene establecer un conjunto de normas que definan también los diferentes niveles de autorización de acceso a los distintos tipos de datos. (iii) Un *plan de acción* para ejecutar estos procedimientos: que debe comprender un conjunto de controles y procedimientos de auditoría que aseguren el cumplimiento continuo de las regulaciones gubernamentales en materia de protección de datos").

[585] Vid. Oñate, J. La clave para compartir información del sector público. *Revista Dintel* número 34. Recuperado de http://www.revistadintel.es/Revista1/DocsNum34/PersEmpresarial/Onate.pdf . En Puyol, J. (20 de noviembre de 2016). ¿Qué es el "Data Governence o gobernanza de los datos"? *Confilegal*. Ahora bien, me parece interesante que abordemos por ejemplo las figuras que participan en los procesos de "data governance" tal y como las que señala OÑATE: "a). *Los patrocinadores ejecutivos* que incluyen el más alto nivel de gestión de la organización. Ellos proveen los recursos y la financiación, incluyendo formación, tecnología y servicios. Los patrocinadores ejecutivos deben tener acceso a las métricas de calidad de datos, análisis de correlación e indicadores clave de rendimiento. b). *Los miembros del Comité de datos*, entre los que se incluyen a los directores de las unidades de negocio, cuyas responsabilidades son definir las políticas y procesos, y los roles y responsabilidades de los administradores de datos. Deben tener visibilidad sobre el rendimiento para ayudar a afinar las políticas y procesos existentes. c). Los

En este contexto surge la necesidad de buscar soluciones desde un enfoque global y multidisciplinar dentro de la organización por medio de, por ejemplo, la creación de un *"compliance comitte":*

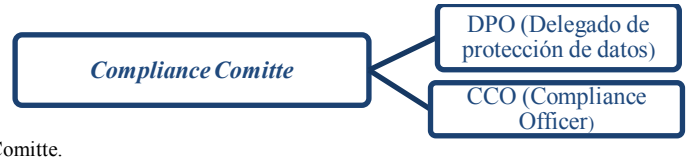


Tabla 32. Compliance Comitte.

La función del Comité será priorizar las áreas de riesgo, acordar las medidas adecuadas y revisar la gestión de riesgos de una manera conjunta. También en este comité se podrá diseñar los códigos éticos o de conducta o *guidelines.*

i. El *DPO* ("*Data Protection Officer")* es exactamente un **experto en protección de datos con un marcado carácter jurídico (o no tanto)**, que se encarga de supervisar el tratamiento de datos personales y asesorar a empresas y organismos públicos en materia de protección de datos, a fin de evitar los riesgos relativos al tratamiento de la información, así como a **evitarles** cualquier tipo de responsabilidad jurídica o **sanciones.** No es una figura nueva en Europa, ya que países como Alemania tenían implantando este perfil desde hace años.

ii. El "*Compliance Officer"* asume la responsabilidad de supervisar los planes de *compliance* orientados a evitar los riesgos de las eventuales responsabilidades penales o de otro tipo que pueden incurrir las personas jurídicas cuando actúan en el tráfico económico. El cargo de *compliance officer* no desdibuja, en ningún caso, el deber de los administradores de control de las compañías ni su potencial responsabilidad en cuanto a que son ellos los que toman las decisiones, sino que personaliza la toma de decisiones a las que corresponde la supervisión del

---

administradores de datos, que son los expertos en los datos que comprende los requisitos de la información. Son responsables de la definición de las reglas de calidad, las definiciones para usuarios no técnicos, la resolución de excepciones y la monitorización de la calidad de los datos. d). Los *analistas*, que capturan y traduce los requisitos de negocio y especificaciones técnicas. Colaboran con los desarrolladores y administradores de datos y forman parte del mantenimiento continuo de la reglas y definiciones de calidad de los datos. e). Los d*esarrolladores* son responsables de la implementación de los requisitos de transformación, pies y gestión de datos de referencia. Se deben evitar las prácticas de integración ad hoc y la codificación manual, ya que es una práctica arriesgada que pueda retrasar los resultados. f). Y finalmente, los llamados "*arquitecto de datos y aplicaciones*", que son los responsables de la definición de los estándares de estructuras, así como los modelos de datos empresariales que permite compartir con éxito los datos".

funcionamiento y cumplimiento del *modelo de prevención* con poderes de iniciativa, que no de decisión. El *compliance officer no deja de ser un oficial o directivo auxiliar*, sin poderes ejecutivos, que participa en el diseño, implementación, verificación y actualización de los programas de cumplimiento. Es más, a diferencia del DPO, al *compliance officer* no le corresponde ni la adopción ni la modificación de los programas de cumplimiento ni la decisión final en relación con los mismos; solo ostenta poderes de iniciativa y de control[586].

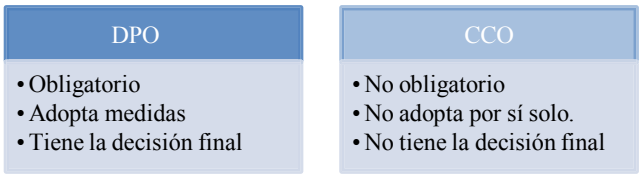


Imagen 33. Diferencias entre DPO y CCO.

2. AUTORREGULACIÓN

Es de sobra conocida la dificultad de conciliar el avance tecnológico con la legislación. El escenario en el que nos encontramos se evidencian dos problemas: la lentitud de la máquina legisladora y la dificultad para el legislador de entender la complejidad tecnológica. Como veremos los diferentes mecanismos de autorregulación procurarán evitar, anticipar, completar y estandarizar la legislación compensando insuficiencias y limitaciones, sobre todo en ámbitos tecnológicos[587] donde se ven afectos los derechos fundamentales y libertades de las personas. Para ello, se integrarían dentro del régimen jurídico "normas *de facto*" a través de lo que se conocía cómo códigos deontológicos (que ahora es algo más que eso). En todo caso, la autorregulación y el marco normativo coexistirán y se complementarán entre sí. Durante el desarrollo de estos, varios miembros *("stakeholders")* de un sector, industria, organización o

[586] La intervención de estas figuras (teniendo en cuenta la obligatoriedad y otras circunstancias) resulta muy adecuada para la consecución de los objetivos y alcanzar el cumplimiento normativo en materia de protección de datos. Además, quisiera destacar algunas ideas que destaca el profesor Puyol: (i) Se requerirá del compromiso de los altos mandos o dirección de la organización en la implementación de las políticas de esta naturaleza; (ii) las políticas irán acordes a los criterios de cultura y de estructura organizativa. Conceder demasiada importancia a la seguridad, puede perturbar una adecuada gestión de datos; (iii) las políticas de las que hablamos tienen que estar diferenciadas del resto con una permanencia estable y continuada en el tiempo. Además, se adaptarán a medida que lleguen cambios, nuevas informaciones y volúmenes de datos y tendrán un carácter formal.

[587] Las tecnologías emergentes como cloud, big data, IoT, blockchain, etc. inevitablemente impactarán en los derechos y libertades de las personas, de ahí que los stakeholders implicados deberán participar en su desarrollo para generar confianza. para lograr generar confianza.

institución (pública o privada), asociaciones, gobiernos, usuarios y titulares de datos[588] interactuarán y darán su voz.

A continuación, hablaremos de los *best practices corporativas*, de los códigos tipo de conducta y de los sectoriales tecnológicos. La adhesión a todos ellos supondrán ahora un medio de prueba o elemento acreditativo de "accountability" y de "compliance" para responsables del tratamiento frente a terceros (clientes, proveedores, competidores, autoridades de control, público) y que además servirán para el "proceso de homologación" de proveedores tecnológicos.

2.1.Código- tipo de conducta

2.1.1. Derecho nacional

Según Rubí[589] (AEPD, 2000), " los códigos tipo son códigos deontológicos o de buena práctica profesional elaborados por los responsables del tratamiento de datos personales para ampliar o facilitar el cumplimiento de las obligaciones establecidas en la normativa sobre protección de datos personales, incrementar las garantías de los ciudadanos y el ejercicio de sus derechos, reforzar las estructuras organizativas y técnicas en el tratamiento de aquellos y, en particular, las medidas de seguridad; o contemplar procedimientos específicos para la tutela de los principios y derechos exigibles en esta materia"

Con la antigua LOPD, los códigos tipo en materia de protección de datos personales podían adoptar alguna de las siguientes formas (145.2 Reglamento LOPD); (i) de ámbito privado individual; (ii) de ámbito privado sectorial (por ejemplo, Farmaindustria[590] o la unión catalana de hospitales); (iii) de ámbito público individual (UCLM); y (iv) de ámbito público sectorial (Asociación Municipios Vascos). En la actualidad hay 15 códigos (salvo error); una cantidad escasa teniendo en cuenta que han transcurrido casi dos décadas. Por lo que hasta el momento se podría decir que los

[588] En la actual LOPDGDD, no obstante y salvo error, no se encuentra mención expresa por parte del legislador a algún periodo de "consulta pública" como el que existía en el art. 147.1. del Reglamento de la LOPD, en el cual se pudiera realizar *alegaciones.*

[589] Rubí, J. (2000). Los códigos tipo: la alternativa de la autorregulación. *Revista Actualidad Informática Aranzadi*, 35.

[590] Nanopdf (19 de marzo de 2018). *Código TIPO sectorial de Investigación Clinica y Farmacovigilancia.* Recuperado de https://nanopdf.com/download/codigo-tipo-sectorial-de-investigacion-clinica-y-farmacovigilancia_pdf

códigos de conducta privados sectoriales son mayoritariamente utilizados en nuestro país. En preciso señalar la intencionalidad. ausente de carácter vinculante, que tenía el legislador en la antigua LOPD ; "tendrán el *carácter de códigos deontológicos* o de *buena práctica profesional*" [591].

Respecto al proceso, podemos encontrar indicaciones del legislador (no sencillas a priori por las numerosas remisiones) en la LOPD-GDD (art. 38)[592]. Es decir, si antes del RGPD, la AEPD era quien aprobaba o no un código de conducta (sin llegar a corregirlo o instar recomendaciones), en la actualidad nuestra AEPD "delega" (sin perder facultades) la supervisión del código de conducta en un organismo acreditado. Posiblemente será una cuestión a tratar en el futuro reglamento de la actual LOPD.

2.1.1.1. Código Farmaindustria.

La Asociación empresarial de la Industria Farmacéutica creó un grupo de trabajo donde analizarían la aplicación de la normativa sobre protección de datos personales. En 2009, se apropó el Código Tipo de la Asociación integrando a más de 200 laboraratorios (85%) de las ventas en España. Las ventajas que aportarían entre otras son;

---

[591] Ahora bien, ¿quiénes los promoverán? El considerando 76 del actual RGPD establece:"se debe incitar a las *asociaciones u otros organismos* que representen a *categorías de responsables del tratamiento* a que elaboren códigos de conducta, dentro de los límites fijados por el presente Reglamento, con el fin de facilitar su aplicación efectiva, teniendo en cuenta las *características específicas del tratamiento* llevado a cabo en determinados sectores". Por tanto, el legislador se refiere a "Estados miembros, las autoridades de control, el Comité y la Comisión" (art.40 RGPD). No obstante, se pensaba que desde la aprobación del RGPD en 2016 se aprovecharía a promover en mucha mayor medida este nuevo instrumento por parte de la Autoridad de control y del Estado pero en verdad, eso parece no haber ocurrido a día (al menos en la medida que se esperaba), pero podemos mencionar algunos ejemplos de gran interés y que afectan a nuestro campo de estudio.

[592] Señala que "3. Los códigos de conducta *serán aprobados por la Agencia Española de Protección de Datos* o, en su caso, por la autoridad autonómica de protección de datos competente. 4. La Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos someterán los proyectos de código al *mecanismo de coherencia* mencionado en el artículo 63[592] de Reglamento (UE) 2016/679 en los supuestos en que ello proceda según su artículo 40.7. El procedimiento quedará suspendido en tanto el Comité Europeo de Protección de Datos no emita el dictamen al que se refieren los artículos 64.1.b) y 65.1.c) del citado reglamento. Cuando sea una autoridad autonómica de protección de datos la que someta el proyecto de código al mecanismo de coherencia, se estará a lo dispuesto en el artículo 60 de esta ley orgánica. 5. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán *registros[592] de los códigos de conducta* aprobados por las mismas, que estarán interconectados entre sí y coordinados con el registro gestionado por el Comité Europeo de Protección de Datos conforme al artículo 40.11 del citado reglamento. El registro será accesible a través de medios electrónicos. 6. Mediante real decreto se establecerán el contenido del registro y las especialidades del procedimiento de aprobación de los códigos de conducta".

- Los laboratorios farmacéuticos dispondrán de *protocolos de actuación* que permitirán la aplicación de criterios uniformes en el tratamiento de datos de sujetos en *supuestos de investigación clínica y farmacovigilancia* con datos de carácter personal y con datos disociados.
- Los sujetos participantes tendrán las máximas garantías en el tratamiento de sus datos.
- En materia de farmacovigilancia, se pretenderá responder de manera uniforme y adecuada a los múltiples escenarios que pueden darse en el proceso de comunicación de acontecimientos adversos y en la obtención del *consentimiento informado.*
- Se otorgará mayor seguridad y certidumbre jurídica a la hora de interpretar normativa vigente (en aquel momento LOPD y RLOPD derogados) para laboratorios e Industria Farmacéutica, en general. Se entiende que deberá ser actualizado habida cuenta el RGPD y en su caso, la nueva LOPDGDD.

El código será de aplicación a; (i) los laboratorios farmacéuticos asociados a Farmaindusria que quieran adherirse; (ii) los laboratorios farmacéuticos no asociados; (iii) organizaciones de investigación por contrato (también los que presente servicios en materia de farmacovigilancia) que presten servicios por cuenta de laboratorios para los estudios en los que sean promotores y manifieste de forma expresa la adhesión. En definitiva, dentro del ecosistema formado por investigadores, promotores, centros hospitalarios, auditores y colaboradores se pretenderá que todos ellos cumplan las obligaciones de código tipo.

En cualquer caso, se aplicará sobre (i) las investigaciones clínicas que usen datos personales o disociados y se extenderá a cualquier tipo de soporte y modalidad de tratamiento automatizado o no; (ii) la farmacovigilancia con datos personales o con datos disociados , los cuales se referirán a acontecimientos adversos relacionados con el consumo de productos comercializados por los laboratorios; (iii) los ficheros de investigación clínica, el fichero de cuadernos de recogida de datos y el fichero de farmacovigilancia.

El código tipo tiene 4 protocolos de actuación; (i) el protocolo de actuación en ensayos clínicos y otras investigaciones clínicas donde habrán reglas específicas sobre la recogida de los datos, el consentimiento informado, etc; (ii) el protocolo de actuación de farmacovigilancia (derechos sujetos, medidas de seguridad, transferencias internacionales); (iii) protocolo para la atención de derecho de sujetos

en investigación clínica y farmacovigilancia con datos personales y disociados con 7 anexos de modelo de solicitud y respuesta; (iv) protocolo de actuación del sistema de autorregulación que tiene por objeto fijar el procedimiento para supervisión por parte de Farmaindustria, articulando medios de comunicación con la propia AEPD.

2.1.2. Derecho comunitario.

Desde 2016 existe un *código de conducta sobre privacidad de las aplicaciones de salud móviles*[593] que permite a los desarrolladores adherirse al mismo y de esta manera, adquirir compromiso voluntario con los usuarios (e-pacientes) en el cumplimiento del la RGPD. Este código de conducta podría responder a las necesidades de autorregulación del ámbito de desarrollo de apps de salud motivada por la preocupación de los usuarios conscientes de la importancia de la privacidad de su datos más delicados: los de la salud. Las cuestiones que tratan tienen que ver con lo contenido en la normativa: el consentimiento del usuario, la limitación de propósito y minimización de datos, la privacidad por diseño y por defecto, los derechos de los sujetos de datos y requisitos de información, la retención de datos, las medidas de seguridad, los principios sobre la publicidad en las aplicaciones *mHealth*, el uso de datos personales para fines secundarios, la cesión de datos a terceros, las transferencias de datos, la violación de datos personales, y datos recogidos de los menores (art. 40.2.g).

2.1.3. Derecho comparado. Caso Reino Unido.

Fuera de España, podemos mencionar al código de conducta 2018 del Gobierno inglés y el Departamento de Salud y Asistencia Social y NHS el cual dejaron expuestos al público para recibir comentarios al igual que colaboraciones de académicos, expertos de la industria, reguladores y organizaciones representativas de pacientes. Con éste, se pretende que se cumplan los principios éticos para las iniciativas de datos desarrolladas por el *Nuffield Council on Bioethics (2015)*[594].

[593] Comisión Europea (7 de junio de 2016). Digital Single Market. *Code of Conduct on privacy for mHealth apps has been finalised.* Recuperado de https://ec.europa.eu/digital-single-market/en/news/code-conduct-privacy-mhealth-apps-has-been-finalised

[594] *Supra cit.*

Como nos podemos dar cuenta se da bastante importancia a la transparencia de los algoritmos, de los fines comerciales y de preservar el interés último del titular del datos frente a éstos anteriores. Posiblemente responden a calmar el revuelo que originaron proyectos como *Deep Mind Health*[595].

2.2.Autorregulación privada sectorial tecnológica.

Este mecanismo puede resultar muy conveniente, al menos hasta que el sector madure y el legislador no tenga conocimientos técnicos que requiere una regulación tan específica y concreta como la que se necesita[596].

Resulta interesante ver de qué principios se tratan:

i. Comprender *a los usuarios,* sus necesidades y el contexto.
ii. *Definir el resultado y cómo la tecnología* contribuirá a ello.
iii. Use datos que estén en línea con las pautas apropiadas para el propósito para el cual se están utilizando. Refiriéndose al principio de minimización, por ejemplo.
iv. *Ser justo, transparente y responsable* sobre qué datos se están utilizando. Refiriéndose a los principios de protección de datos por diseño[594] con acuerdos de intercambio de datos, a los mapas de flujo de datos (en el análisis previo) y evaluaciones de impacto de protección de datos (EIPD) y demás aspectos de la ley de la protección de datos de 2018.
v. Hacer uso de *estándares abiertos*. Señala concretamente: "Utilice y construya en el producto o la innovación los datos actuales y los estándares de interoperabilidad para garantizar que pueda comunicarse fácilmente con los sistemas nacionales existentes".
vi. Ser *transparente* sobre las limitaciones de los datos utilizados y *los algoritmos implementados*. Señala concretamente: "Comprenda la calidad de los datos y considere sus limitaciones cuando evalúe si es apropiado para las necesidades de los usuarios y el contexto. Al crear un algoritmo, sea claro acerca de sus fortalezas y limitaciones, y brinde evidencia clara de si el algoritmo que ha publicado es el algoritmo que se usó en la capacitación o en la implementación".
vii. Mostrar qué *tipo de algoritmo* se está desarrollando o implementando, el examen ético de cómo se utilizan los datos, cómo se validará su desempeño y cómo se integrará en la provisión de salud y atención.
viii. Generar evidencia de *efectividad* para el uso previsto y la relación calidad-precio.
ix. Hacer *seguridad* integral *al diseño*.
x. Definir la *estrategia comercial*. Se cita: "Considere *solo* la posibilidad de entrar en términos comerciales en los que los beneficios de las asociaciones entre las compañías de tecnología y los proveedores de salud y atención se compartan de manera justa".

[595] Stolker-Walker, C. (14 noviembre 2018). Why Google consuming DeepMind Health is scaring privacy experts. *Wired.* Recuperado de https://www.wired.co.uk/article/google-deepmind-nhs-health-data

[596] Desde el inicio de este trabajo, existían varias premisas claras que hicieron de base para poder iniciar el proyecto. Una de ellas era que la autorregulación *"privada"* sectorial se iría asentado hasta que los reguladores pudieran poner en marcha la maquinaria normativa en materia de protección de datos y las diferentes tecnologías (cloud, big data, IA, IoT y blockchain) maduraran en el mercado. El objeto de la autorregulación radica en la reducción de costes de transacción, puesto que para la Administración Pública sería más costoso recolectar información para generar regulación (y si lo hiciera, correría el peligro de que fuera ineficiente). La sanción del mercado por no actuar éticamente o fuera de ciertos estándares mínimos de conducta puede ser mucho más severa que aquella que pueda imponer la Administración. A continuación citemos algunos ejemplos de este mecanismo.

En primer lugar, a nivel nacional, la asociación *Eurocloud* que surge con el ánimo de poder establecer un marco de buenas prácticas y posibilitar la homologación a través de su sello de calidad, prevenir sanciones y reclamaciones judiciales. El procedimiento consistirá en la adhesión a las clausulas estándar en materia de protección de datos posibilitando que éstas se puedan introducir en los documentos contractuales y de esta manera se podría recibir un "sello de certificación" [597]. En segundo lugar, a nivel comunitario, se encuentra la *CISPE*[598][599] o *Coalición de proveedores de infraestructuras de cloud computing en Europa* como primer código de conducta europeo y fundada por *Sky Skyscape Cloud Services* (Reino Unido), *OVH* (Francia), *Ikoula* (Francia), *Aruba* (Italia), *Hetzner* (Alemania) and *Amazon* (Estados Unidos). Su código de conducta relativo a la protección de datos, permitirá a los clientes identificar fácilmente si el tratamiento de los datos personales que realizan sus proveedores se adapta a sus necesidades de confidencialidad y seguridad. Por su parte, Cloud Security Alliance (CSA) y ENISA (Agencia de Seguridad de la Información) promueven e incentivan el uso de las best practices (también, en cloud) para ofrecer garantías de seguridad.

A efectos prácticos, el cliente (hospitales, centros médicos, aseguradoras de salud eHealth, centros de investigación, tecnológicas, industria farmacéutica) podrá

[597] Ver https://revistapymes.es/eurocloud-crea-un-codigo-de-buenas-practicas-para-dar-mayor-seguridad-a-los-usuarios-de-la-nube/

[598] La eurodiputada Eva Paunova, miembro de la Comisión de Mercado Interior y Protección del Consumidor**,** declaró lo siguiente: "Como legisladores, nosotros podemos elaborar un proyecto de ley perfecto en papel, pero la clave está en saber que este proyecto es factible y que puede funcionar en la práctica. En este sentido, recibimos con satisfacción el *Código de Conducta CISPE* que permitirá que los clientes europeos cuenten con la garantía de que sus datos gozan de un alto nivel de protección"

[599] Ver en https://cispe.cloud/code-of-conduct/.
Ver http://www.dealerworld.es/cloud/primer-codigo-de-conducta-europeo-adoptado-por-proveedores-cloud
Los interesantes objetivos de *CISPE* son:

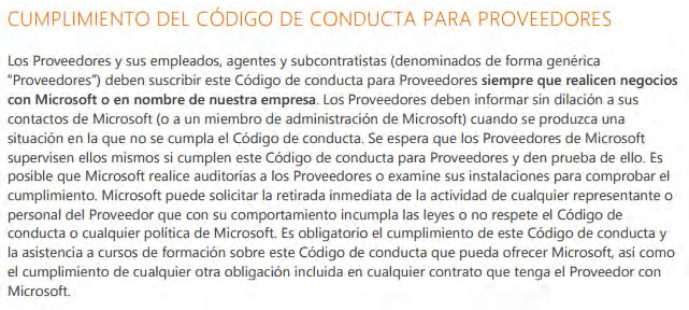
i. "Proponer iniciativas que crean un mercado europeo de la nube única e impulsan el crecimiento de *IaaS.*
ii. Fomentar las iniciativas primeras políticas de contratación pública cloud.
iii. Promover los requisitos de seguridad en toda la UE y estándares.
iv. Fomentar soportes de privacidad incluyendo un Código de Conducta para la Infraestructura Cloud.
v. Mantener el mercado de IaaS abierto en la UE y libre de *"lock-in"* (uno de los mayores riesgos en cualquier EIPD respecto al derecho de portabilidad).

Oponerse a gravámenes injustificados o a obligaciones de control de contenido y educar en políticas sobre la infraestructura en la nube y deficiencias que afecten a la captación del mercado europeo de cloud".

servirse de ello para evaluar al proveedor candidato *"autorregulado"* gracias a su visibilidad y transparencia en el proceso de homologación[600].

2.3.Best practices corporativas.

La autorregulación[601] podrá ser "*intra cumplimiento*" y desarrollarse en el contexto de una organización y terceros (subproveedores, clientes, etc.). Lo más frecuentes es que se extienda en todo el contexto de la cadena de suministro de los propios proveedores tecnológicos, es decir, también abarcando a los subproveedores. Por ejemplo, *Microsoft* obliga a la adhesión a su código de conductas (al igual que a su asistencia formativa)



CUMPLIMIENTO DEL CÓDIGO DE CONDUCTA PARA PROVEEDORES

Los Proveedores y sus empleados, agentes y subcontratistas (denominados de forma genérica "Proveedores") deben suscribir este Código de conducta para Proveedores **siempre que realicen negocios con Microsoft o en nombre de nuestra empresa**. Los Proveedores deben informar sin dilación a sus contactos de Microsoft (o a un miembro de administración de Microsoft) cuando se produzca una situación en la que no se cumpla el Código de conducta. Se espera que los Proveedores de Microsoft supervisen ellos mismos si cumplen este Código de conducta para Proveedores y den prueba de ello. Es posible que Microsoft realice auditorías a los Proveedores o examine sus instalaciones para comprobar el cumplimiento. Microsoft puede solicitar la retirada inmediata de la actividad de cualquier representante o personal del Proveedor que con su comportamiento incumpla las leyes o no respete el Código de conducta o cualquier política de Microsoft. Es obligatorio el cumplimiento de este Código de conducta y la asistencia a cursos de formación sobre este Código de conducta que pueda ofrecer Microsoft, así como el cumplimiento de cualquier otra obligación incluida en cualquier contrato que tenga el Proveedor con Microsoft.

Imagen 64. Código de conducta de proveedores de Microsoft. Fuente: Microsoft[602]

Me gustaría hacer una observación. Con el código de *Microsoft* en la mano, nos podemos preguntar "¿por qué no incluir un apartado similar y expreso como el de "protección de activos y propiedad intelectual" (pág. 4-5) que se denomine "protección de datos personales"? Incluso, ¿por qué no hacer referencia expresa a categoría de datos como son los datos personales de la salud y a sus particularidades, estableciendo la obligatoriedad del cumplimiento de determinadas medidas técnicas y organizativas que garantice que en la cadena de suministro cloud desde el inicio hasta el último subproveedor cumple con la normativa y con el código de conducta?. E incluso, ¿Por

[600] Desde el inicio de este trabajo, existían varias premisas claras que hicieron de base para poder iniciar el proyecto. Una de ellas era que la autorregulación *"privada"* sectorial se iría asentado hasta que los reguladores pudieran poner en marcha la maquinaria normativa en materia de protección de datos y las diferentes tecnologías (cloud, big data, IA, IoT y blockchain) maduraran en el mercado.

[601] Pérez Campillo, L. (2017). Códigos de conducta y best practices en cloud computing. Recuperado de https://blogs.itdmgroup.es/lorena-p-campillo/2017/01/codigos-de-conducta-y-best-practices-en-cloud-computing-lo-que-esta-por-llegar

[602] Vid.http://download.microsoft.com/download/F/9/9/F998F8EB-038A-4EEE-8B36-4B87362DBE96/Spanish_Spain.pdf

qué no señalar en ese apartado hipotético vías de contacto del DPO para canales de denuncias ante comportamientos dudosos?[603].

3. CERTIFICACIÓN.

El certificado de privacidad se realiza a través de un procedimiento opcional, imparcial, transparente y tiene como objetivo principal facilitar un *aumento de la transparencia u confianza del mercado* respecto a la privacidad y la protección de datos. Además aportarán valor competitivo al fortalecer la imagen corporativa e innovador, dado su carácter anticipador a los cambios legislativos. Así por ejemplo, el grupo *C-SIG CERT* que surge a raíz de la estrategia digital del mercado único de 2015 y que fue establecido con el apoyo de la Red de la Unión Europea y ENISA establecieron una posible lista de certificados "voluntarios" a disposición de los clientes cloud para posibilitarles más transparencia e información[604]. Sin embargo, a pesar de su buen trabajo, estas organizaciones parece no ofrecer estándares a día de hoy con amplia aceptación en el mercado para que ofrezcan soporte a la adquisición de servicios, creación de contratos y negociaciones. De hecho, algunos proveedores[605] reconocen que adquirir las certificaciones oficiales puede ser un *proceso caro y complejo*, máxime si éstas quedan *invalidadas* después de posibles cambios o actualizaciones del software o hardware al quedar desactualizados o evolucionados o que incluso no son lo suficientemente eficaces[606].

3.1.Sellos de privacidad

3.1.1. El sello europeo de privacidad ("European Privacy Seal").

[603] Vid. https://www.youtube.com/watch?v=1K5Ji_Kf1F8

[604] Vid https://resilience.enisa.europa.eu/cloud-computing-certification.

[605] Vid. Kuan Hon, W., Millard, C. Walden, I. (2012). Negotiating cloud contracts: Looking at clouds from both sides now. *Standford Technology Law Review.* Vol. 16. Number 1. Recuperado de http://stlr.stanford.edu/pdf/cloudcontracts.pdf. (Algunos proveedores tal y como recoge la investigación de la Revista de la Universidad de Standford, varios proveedores reconocen el problema de desconfianza de la seguridad, pero señalan que tras el ejercicio de diligencia debida de sus clientes poniendo en marcha certificaciones como las PCI/DSS[605], ISO27001 y SAS7076 , pudieron confiar en el proveedor).

[606] Como es el caso del Gobierno de Reino Unido y el sector público, donde el CESG (Programa de Subvención para la garantía de la Información) aseguró que "*VMware vSphere 4.0* contaba con un marco de protección restringida (no suficiente) con solo un nivel 3 para acoger en la misma plataforma, información del sector público. Siendo el "Nivel 3: Puede potencialmente causar una pérdida financiera para la HMG / Sector Público de hasta 1 millón de £. Es probable que provoque una pérdida financiera significativa para ninguna de las partes - por ejemplo, bajo 10,000.00 £ para un comerciante individual o única o bajo 100.000,00 £ para un negocio más grande". Vid. http://www.cesg.gov.uk/Publications/Documents/cesg-vmware_joint-statement14-09- 11.pdf

EuroPriSe[607] se inició como un proyecto financiado por la UE destinado a establecer una sello de red transeuropea y ahora ofrece certificaciones para productos de TI, servicios basados en TI y sitios web en la UE. El sello asegura a los usuarios que sus datos se manejan de acuerdo con las leyes europeas de protección de datos. Estas han sido otorgadas a empresas de todos los tamaños, incluidas las pequeñas y medianas empresas, así como las organizaciones multinacionales como *Microsoft, SAP y Siemens.* Otros ejemplos son *Quentry* el cual fue la primera empresa de servicio médico en cloud en obtener el sello y como proveedor cloud permite anonimizar los datos clínicos a profesionales, clientes o investigadores o *Ixquick*[608] como metabuscador.

3.1.2. Sellos de privacidad en España[609].

A nivel nacional, e incluso autonómicos ya hay sellos de privacidad para *aplicaciones móviles de salud*

3.2.Certificaciones técnicas.

A continuación, mencionamos las siguientes;

---

[607] El sello certificará que los proveedores tecnológicos **cumplen con la normativa europea de protección de datos. Las fases del procedimiento son : (i)** *Fase de Evaluación.* Los expertos realizarán verificaciones legales, técnicas y de la documentación y los resultados conseguidos se reflejan en un informe de evaluación confidencial; (ii) *Fase de Validación.* El siguiente paso es la presentación del Informe de Evaluación al Organismo Certificador, el cual repasará la metodología, la congruencia y la honradez del informe, que podrá ser validado, rechazado o puede exigir explicaciones adicionales; (iii) *Obtención del Sello.* Una vez aprobado el Informe de Evaluación por ese Organismo Certificador, el Sello será concedido en acto público en una capital europea. Será a partir de ese instante cuando el servicio cloud se encuentra certificado. El periodo aproximado para la obtención de la resolución está entre 3 y 5 meses, dependiendo de la dificultad del proyecto y de la cantidad de información adicional o aclaraciones que pudiera pedir el Organismo Certificador. El RGPD obligó a *EuroPriSe* a iniciar una actualización de sus criterios de certificación y la Autoridad de Certificación EuroPriSe (CA) aprovechó la oportunidad para ajustar el catálogo. Ahora bien, ¿podrán estar al alcance del presupuesto de start up de health teniendo en cuenta que la tasa ronda los 10.000 euros? . Ver https://www.european-privacy-seal.eu/EPSen/Criteria.

[608] La privacidad está garantizada por el uso de varias técnicas de minimización de los datos: los datos personales como direcciones IP se eliminan dentro de las 48 horas, después de lo cual ya no son necesarios para evitar un posible abuso de los servidores. Los datos restantes (no personales) se eliminan dentro de los 14 días. Ver https://www.ixquick.com/esp/press/eu-privacy-seal.html?hmb=1

[609] Vid. https://www.juntadeandalucia.es/agenciadecalidadsanitaria/informe/2018/T3/centros/AppAPP.html donde ya 23 tienen el mismo (Vid. http://www.calidadappsalud.com/distintivo/catalogo)y otras está en proceso como *Social Diabetes.*

3.2.1. ISO 27001.

Se trata de un sistema de gestión , más bien orientado a la seguridad y proporciona requisitos específicos para ello se requerirá de una auditoría.

3.2.2. ISO 27018.

Establece los objetivos de control y directrices para medidas de "protección de información de identificación (PII)" (o datos personales) , de conformidad con los principios de privacidad y es aplicable a todos los tipos y tamaños de organizaciones, incluidas las empresas públicas y privadas, entidades gubernamentales y organizaciones sin fines de lucro, que proporcionan servicios de procesamiento de información como encargados de tratamiento de datos personales a través de cloud computing bajo contrato con otras organizaciones. Esta norma tiene muy presente la normativa europea y el inminente reglamento europeo de protección de datos. El problema se encuentra en el difícil ensamblaje entre la normativa técnica y la heterorregulación pública por parte de la Unión Europea, la Comisión Europea o los Estados miembros. Microsoft fue el proveedor cloud que primero adquirió esta certificación internacional pero su adhesión no implica que cumpla con la normativa española. Lo que sí garantiza al menos es la transparencia en la ubicación de la información almacenada y medidas de seguridad para la eliminación de la misma. Microsoft tiene diferentes instrucciones en función del tipo (Microsoft Azure, Intune, Dynamics CRM Online u Office 365)[610] .

3.2.3. ISO 19086-1.

Tiene por objeto proporcionar una orientación común sobre lo que debe incluirse en el CSA (contrato de servicio de nube). La norma ayudará a abordar el problema de la capacidad de negociación porque las organizaciones pueden apuntar a la norma como un punto de referencia para lo dispuesto en el CSA debe contener. EL documento podrá ser utilizado por cualquier organización o individuo implicado en la creación, modificación o comprensión de un acuerdo de nivel de servicio en la nube que se ajusta a la norma por su fácil comprensión[611].

3.2.4. IEC 27552.

El objetivo es mejorar el Sistema de gestión de seguridad de la información existente con requisitos adicionales para establecer, implementar, mantener y mejorar continuamente un Sistema de gestión de información de privacidad. El borrador de la norma describe un marco para responsables de tratamiento y los encargados para administrar los controles de privacidad a fin de reducir el riesgo de los derechos de privacidad de las personas. Si bien la norma aún se encuentra actualmente en borrador, pretende ser una extensión certificable a las certificaciones ISO / IEC 27001[612].

3.2.5. Cobit 5.

[610] Vid. https://www.microsoft.com/es-xl/TrustCenter/Privacy/You-are-in-control-of-your-data
[611] Vid. https://www.iso.org/obp/ui/#iso:std:iso-iec:19086:-1:ed-1:v1:en
[612]Vid.https://en.wikipedia.org/wiki/ISO/IEC_27552 y https://www.linkedin.com/feed/update/urn:li:ugcPost:6494233359500345344/

Es el marco de referencia de ISACA[613] para el gobierno corporativo y la gestión de IT de la empresa.

3.2.6. Staraudit.

Es un programa global orientada a la tecnología de cloud computing. Se trata de la certificación de EuroCloud Europe donde una de las áreas de actividad son generar confianza, concienciación, cumplimiento normativa en privacidad, armonización y estándares[614][615].

4. HOMOLOGACIÓN.

Homologación viene del verbo homologar, que significa "*aprobar o confirmar oficialmente"*. Es el proceso de certificación o aprobación de un producto para indicar que cumple con las normas y especificaciones reguladoras, como la seguridad y los requisitos técnicos. Las certificaciones de homologación se conceden por una organización o asociación empresarial, por un organismo oficial o por un tribunal de Justicia. La homologación de proveedores y subcontratistas tecnológicos como la oportunidad para *"filtrar"* a los proveedores que cumplen los criterios fijados del cliente en relación con la normativa de protección de datos aparece de los que no. O en otras palabras, la homologación evita costes y tiempo en reuniones poco fructíferas entre departamentos jurídicos. El proceso se concibe como una transición de estado (de un sistema no homologado a homologado). A continuación describimos las que podrían ser unas posibles fases para esa homologación donde los *parámetros* podrían ser varios en función del tipo de "homologación" utilizada y los criterios deseados del cliente:

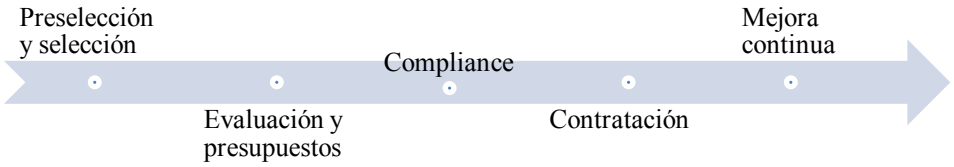


Table 34. Fases posibles de homologación

[613] Es una asociación independiente sin fines de lucro que cuenta con más de 140,000 profesionales de gobierno, seguridad, riesgos y aseguramiento en 187 países.
[614] Vid. https://eurocloud.org/streams/staraudit/
[615] Ahora bien, después de haber repasado algunos ejemplos de certificación técnica cabe preguntarnos; ¿cuál será su futuro? Es pensable que la futura normativa técnica que apruebe la Comisión o cada EEMM tendrá conexión estrecha con la normativa técnica privada que se va desarrollando en las diferentes tecnologías. La realidad es que muchos EEMM que deberían regular aspectos técnicos y concretos de tecnologías (como cloud, IoT, o blockchain) no lo están haciendo. Por lo que ante en escenario de posible vacío e indefinición normativa, el papel de la normativa técnica privada se torna imprescindible.

a. **Preselección y selección de proveedores tecnológicos.** La empresa cliente de los servicios tecnológicos, definirá y desarrollará los objetivos y criterios de los proveedores. El equipo de gestión de proveedores o departamentos de compras y el departamento jurídico suelen encargarse de esa búsqueda pero lo adecuado sería armar un equipo multidisciplinar posible evaluador como el siguiente:

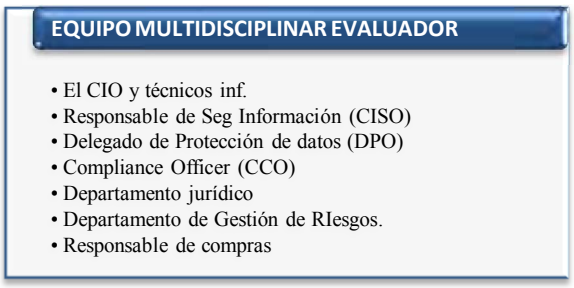


Tabla 35. Miembros del equipo multidisciplinar evaluador[616].

Dada la particularidad de los servicios Cloud, habrá que añadir los siguientes requisitos importantes:

b. **Evaluación y presupuesto.** En concreto, se referirán a si superan los criterios legales que pueden ser : (i) tenencia de *certificaciones*[617]*; (ii)* adhesión al *códigos de conducta*; (iii) *flexibilidad contractual* (acuerdos); (iv) cláusulas de confidencialidad y (v) c*umplimiento RGPD/LOPDGDD*.

c. **Fase de compliance que implica los correspondientes checklist, el cuestionario de compliance, la comprobación de las certificaciones, etc. De la fase de compliance, se pasa a la de contratación.**

d. **Contratación. En esta fase se revisará el contrato, después se firmará el contrato, del código de conducta, y de las condiciones generales de contratación, el PLA y demás aspectos determinantes.** El departamento jurídico no debe esperar hasta el último momento para repasar los términos contractuales.

e. **Mejora continua.** La homologación es temporal y requiere de evaluación continua que se basa fundamentalmente en la detección y en las medidas correctoras o la gestión del incumplimiento. En el caso de las iniciativas de detección y control, se basa la política en *auditorías periódicas*, tanto internas como de independientes. Si es un proveedor crítico para la organización, se analizan los

[616] Como se puede ver dentro de ese equipo participa el DPO (externo o interno de la empresa). Ahora bien, una vez definidos los objetivos y criterios de evaluación, el cliente seleccionará la lista de proveedores a los cuales se les aplicará el programa, y por tanto, los que recibirán las auditorías. En esta etapa se enviarán cierta información (como cuestionarios estándar) que deben cumplimentar o aportar a los proveedores preseleccionados.

[617] Posesión de estándares internacionales en materia de seguridad de información (ISO 27001, 27002 y 27018) o adhesión a estándar internacional (ISO28000) de calidad en la cadena de suministro. Posesión de *certificación calidad* (ISO 9001). Art. 7.4 (Gestión de proveedores). ISO 14001, OHSAS 18000.

motivos de la evaluación negativa y se plantean iniciativas para *potenciar las áreas de mejora* identificadas que incluyen, entre otras, actividades de formación y colaboración.

Ahora bien, me surgen interrogantes como; ¿permitirán empresas como Microsoft ser auditadas? Podemos entender por su información pública que la respuesta es negativa. Microsoft se justifica de esta manera: "Si se permitiera a miles de clientes realizar auditorías de nuestros servicios, la práctica no sería escalable y se pondría en peligro la seguridad". No obstante, el programa de confirmación de terceros de *Microsoft* 365, por ejemplo, incluye *auditorías independientes* que se realizan anualmente para confirmar el nivel de seguridad, pero no personalizadas por el propio cliente[618].

5. COMPLIANCE

Dentro de los sistemas de compliance la protección de datos personales es uno de los ejes centrales en el marco del conjunto de aspectos prácticos a los que las empresas deben (o deberían) enfrentarse habitualmente (Agustina y Blumenberg, 2015, 250) [619].

5.1.Definición y características.

El *compliance*[620] no sólo nace como consecuencia de la llegada de la reforma del código penal sino que tiene que ver con un "*movimiento o una cultura global"*[621] que se ha ido

[618] En el 2012, la ICO, la autoridad de control de protección de datos de R.U., hizo un modelo de *checklist , aunque antiguo puede resultar de referencia para aplicarlo a otras tecnologías aparte de cloud* y a la luz del nuevo RGPD, *y* dirigido a los clientes formado por 5 aspesctos; legal, riesgos, confidencialidad, integridad y disponibilidad. Ver en línea: https://ico.org.uk/media/1540/cloud_computing_guidance_for_organisations.pdf. Pág. 21.

[619] Vid.https://www.academia.edu/11420153/El_Data_Protection_Officer_en_el_marco_de_la_responsabilidad_penal_de_las_personas_jur%C3%ADdicas_Consideraciones_a_la_luz_del_nuevo_Reglamento_Europeo_en_materia_de_protecci%C3%B3n_de_datos . Estos autores señalan algo inminente, la llegada del RGPD y la reforma del CP supondría un cambio de paradigma para los empresas que tendrán que "combinar ambos modelos". Si bien es cierto, que el compliance español posibilitaba cierta flexibilidad (y donde faltan pautas concretas o expresas) a la hora de diseñar el programa con estas novedades normativas se van delimitando y perfilando las responsabilidades y obligaciones de los actores involucrados. El compliance, en definitiva, también observará como riesgo estratégico a aquellos que puedan derivar en infracciones administrativas por infracciones en materia de protección de datos en el contexto de la organización o institución.

[620]Teijeira Rodriguez, Mariano. Legal Compliance: Conceptualización en el marco de la regulación corporativa. En: Estudios sobre el futuro Código Mercantil: libro homenaje al profesor Rafael Illescas Ortiz. Getafe : Universidad Carlos III de Madrid, 2015, pp. 935- 948. ISBN 978-84-89315-79-2. Recuperado de http://hdl.handle.net/10016/2102 . El *compliance* surgió con el ánimo de frenar las actuaciones impunes hasta ahora de las grandes organizaciones amparadas por la extraterritorialidad y su posición "dominante" en el mercado. ¿Qué es el *compliance* corporativo en las Tics? Podríamos definirlo como el conjunto de procedimientos y buenas prácticas incorporados en las organizaciones para

desarrollando en los últimos años. Además, cuenta con factores como son la importancia de la imagen corporativa, las buenas relaciones con los grupos de interés, la transparencia propiciada por los medios de comunicación y de la sociedad de la información, las nuevas expectativas de la sociedad depositadas en las organizaciones, etc. Por tanto, el compliance no sólo tendría que ver con la responsabilidad penal de las personas jurídicas.

Se podría pensar más bien que la función de compliance *tiene que ver más con valores (corporativos)*, *comportamientos y la integridad empresarial* dentro del contexto de una organización, como podrían ser la definición de los límites de comportamiento al personal en materia de gestión de información sensible y protección de datos personales. Esta nueva concepción podría encajar bien con el concepto de *"compliance por diseño"* del profesor PUYOL[622]. Según el autor:

> "Los principios de '*Compliance* por Diseño' pueden ser aplicados a todos los tipos de actuación empresarial, pero deben ser aplicadas con especial vigor a aquellos comportamientos que sean *incardinadles* dentro de los tipos contenidos en el nuevo Código Penal de las personas jurídicas; en aquellas *actuaciones empresariales susceptibles de ser sancionadas administrativamente*, o simplemente, en aquellos que sean *reprobables desde un punto de vista social*."

En términos generales, se podría considerar al "*corporate compliance"* como una *cultura* formada por un protocolo en la que se realiza gestión de riesgos y de prevención, también, en materia de protección de datos que son susceptibles consecuencias jurídicas como sanciones administrativas y que pueden ser reprobables

---

identificar los riesgos legales a los que se podrían enfrentar, y una vez analizados éstos, establecer mecanismos para prevenir, gestionar y controlar los mismos, todo ello en un contexto de las Tecnologías de la Información y Comunicación y las operaciones de tratamiento de información que se realizan en el "mundo online". Estos procedimientos tendrán un marcado perfil ético que debe ser adoptado por las organizaciones en función de su actividad empresarial tecnológica. Pero también, y tal como señala el profesor PUYOL (2019), "supone un protocolo de actuación destinado específicamente a impedir que se pueda utilizar la organización, sus medios y sus recursos en estos nuevos ámbitos de actuación, para la comisión de hechos delictivos" [620]. Por ello, según el autor "en este sentido, también debe ser de aplicación a las nuevas tecnologías lo afirmado con carácter general en la Circular 1/2016 de la Fiscalía General del Estado, cuando se señala, que los programas -de Corporate Compliance- deben ser claros, precisos y eficaces, y desde luego, redactados por escrito" (Vid. https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Circular_1-2016.pdf?idFile=81b3c940-9b4c-4edf-afe0-c56ce911c7af**.)** En este sentido, TEIJEIRA (2015, 943) señalaba que "aunque la atención a la cultura ética debe ser el primero de los esfuerzos empresariales, y todos los componentes de la organización deben demostrar periódicamente que se preocupan por la ética, los valores compartidos, deben demostrar su importancia a través de palabras y acciones coherentes (…)"

[621] Vid. http://ecixgroup.com/el-grupo/compliance-como-una-nueva-forma-de-cultura-corporativa/

[622] Vid. http://ecixgroup.com/el-grupo/hacia-una-nueva-institucion-el-compliance-por-diseno/

socialmente. Y en términos específicos, el compliance se podría relacionar con el respeto de los *derechos legítimos de clientes, proveedores, empleados y accionistas*, siendo de aplicación *tanto para el cliente como para el proveedor tecnológico*[623].

Con la llegada del RGPD se puso de manifiesto la creciente e imparable tendencia en Europa y en España de la importancia *de acreditar o probar* los actos/acciones que se llevan a cabo en la compañía, así como la clara preferencia por modelos adaptados ("*made to measure*") en las organizaciones. Estos nuevos modelos de compliance se caracterizarán por cuestiones como las siguientes:

i. El apoyo de la *máxima dirección* (*"tone at the top")* [624]será imprescindible.

ii. El papel de la *formación* y capacitación del personal será esencial. Según una encuesta de la empresa *Liason*[625], el 85% de los empleados no sienten que su seguridad laboral esté en riesgo por problemas de cumplimiento de la legislación. En la actualidad, los directivos se aseguran que es efectiva proponiendo "pruebas" donde se verifique que han accedido a la lectura de ese código ético y la realización de test. Los resultados de la superación de las pruebas individuales pueden quedar reflejados en informes que sirven de evidencia de responsabilidad proactiva para aquellas organizaciones que son responsables de tratamiento.

iii. La *autoimposición normativa*[626] y la adopción de prácticas sectoriales podría incluirse al margen de los mínimos del RGPD y la LOPDGDD. La coordinación de un comité

[623] El contexto en el que se desarrollaría el programa es particular, debido a características como las que señala el profesor PUYOL: (i) la inmaterialidad de la información que es llevada de forma transparente e instantánea en lugares nada cercanos (ej. pensemos en cloud computing); (ii) la interactividad entre usuario y ordenador; (iii) la interconexión entre dos tecnologías; (iv) la instantaneidad y la rapidez de las redes de comunicación y la informática; (v) los elevados parámetros de calidad de imagen y sonido; (vi) la digitalización; (vii) la mayor influencia sobre los procesos que sobre los productos; (viii) la globalización y penetración en todos los sectores (culturales, económicos, educativos, industriales) y se refleja de forma colectiva en un grupo, sector o país en todo el planeta; (ix) la innovación y cambio constante; (x) la tendencia hacia la automatización de la información en diversas actividades personales, profesionales y sociales; (xi) la diversidad en la utilidad de las tecnologías. La tendencia de futuro posiblemente es que las organizaciones, administraciones públicas, los tribunales definan el contexto y alcance de los programas de compliance habida cuenta el tipo de sector , mercado, modelo de negocio o la actividad. Pensemos por ejemplo, en el compliance en el sector de cloud computing para pymes[623] o el sector de IoT para Smart Cities o el sector de Blockchain en asistencia sanitaria *eHealth* o industria farmacéutica. En cualquier caso, el departamento jurídico de las organizaciones e instituciones deberá funcionar proactivamente y autónomamente y no de forma reactiva como en el pasado cuando recibía instrucciones de altos mandos.

[624] Vid. Concepto "tone from the top" Serie de cuadernos KPMG sobre cumplimiento legal. N3. "Sistemas para la gestión del cumplimiento (CSM)- Parte 1. Pág. 12.

[625]Según http://www.ciospain.es/cloud/el-25-de-los-directivos-no-sabe-quien-es-responsable-de-garantizar-la-privacidad-de-los-datos

[626] Por su porte, la Norma ISO: 19600 trata de un documento internacional que establecerá un referente de buenas prácticas en materia de gestión de *compliance* para la detección y gestión de los riesgos por incumplimientos de las obligaciones legales. No se trataría de una norma rígida y cerrada, sino de una norma que ofrece una metodología común capaz de adaptarse según el perfil, la cultura de cumplimiento, economía, modelo de negocio, etc. La norma incluye recomendaciones en relación a la formación, o "la

compuesto por representantes de las diferentes áreas y *responsables de cumplimiento o compliance committies* (ej. DPO, CCO[627], etc.) para empresas de gran tamaño puede ser necesario. Según Teijeira (2015, 943), "el oficial (responsable) de cumplimiento tiene responsabilidades tanto de *cumplimiento* estricto *senso*, como *éticas* toda vez que para lograr los resultados deseados, tanto la ética como el cumplimiento deben ser horneados en la cultura de la organización"[628].

Este comité conjunto podría realizar actividades como:

a. Revisión del *organigrama*.
b. *Gestión de riesgos* (identificación de procesos y conductas de riesgo, identificación de personas y colectivos en riesgo).
c. Vertebrar *políticas y directrices de cumplimiento*, actividad de control y desarrollo del código ético que deberán llegar a los grupos de interés (proveedores y clientes tecnológicos). Por ejemplo, puede darse el caso de que clientes o proveedores soliciten a terceros la adhesión explicita a su código ético o a iniciativas de renombre como *UN Global Compact* mediante la suscripción de un documento o cláusula. Será necesario que exista una jerarquía en esas políticas, donde se puedan distinguir aquellas de alto nivel. Así por ejemplo, un código ético puede posibilitar la consistencia entre las "políticas" de la empresa pero no es de utilidad sino hay controles. Si bien es cierto, no consiguen una seguridad absoluta, puede conseguir un nivel aceptable y una auditoría anual periódica externa podrá ayudar a focalizar las conductas indeseables e irresponsables.

---

integración del desempeño en compliance en la evaluación del desempeño de los empleados, o la supervisión de los acuerdos de contratación externa para asegurarse de que recogen obligaciones en materia de compliance" (Carbayo, 2015). Vid. https://www.ecixgroup.com/iso-19600-la-hoja-de-ruta-del-cumplimiento-normativo/ . También me parece interesante algo que se señala desde KPMG (Vid https://assets.kpmg/content/dam/kpmg/es/pdf/2018/07/estandares-internacionales-compliance.pdf pp 10) por cuanto nos interesa; "se considera un estándar adecuado para construir superestructuras de vocación transversal, capaces de coordinar diferentes bloques técnicos (privacidad, competencia, prevención penal, etc.). Otro apunte resulta interesante; "es el primer texto en aclarar que las obligaciones de Compliance tanto pueden provenir de obligaciones impuestas o exigidas, como de aquellas otras asumidas voluntariamente". Y otra curiosidad: ya no se utiliza el término "oficial de compliance" para hacer referencia en todo caso a un posible órgano según las características de la organización. Además, podrá ser de aplicación a diferentes sectores, incluyendo las del ámbito privado, público o incluso organizaciones sin ánimo de lucro. También, la consultoría destaca el hecho de que no se hayan incluido términos jurídicos puesto que como señalan, la intención no sería que las organizaciones lo vincularan con leyes u ordenamientos jurídicos.

[627] El profesor Puyol indica de manera acertada algunas de las funciones posibles de un *compliance officer*: "a). Conocer las características que debe tener la política de privacidad y protección de datos personales, y que garantías tiene los derechos digitales en el seno de la empresa.b). Verificar la legalidad de la ética de los sistemas de tratamientos de datos personales. c). Analizar los aspectos que inciden en la legalidad web, y en una Cookie Program. d). Conocer los aspectos relativos a la firma e identificación electrónica. e).Comprender el procedimiento para obtener evidencias electrónicas. f). Entender las cuestiones claves de la ciber seguridad."

[628] *Supra cit.*

d. Implantación de *canales de denuncia* aplicados al RGPD y LOPDGDD donde se informe de posibles riesgos e incumplimientos de las medidas organizativas y técnicas en protección de datos.
e. Creación de *planes de acción.* Se contemplará por un lado, las medidas para gestionar el riesgo y por el otro, las consecuencias que se derivarán a las personas de la organización o colaboradores que los han generado. No obstante, la mera tenencia de la documentación de un modelo (como medida "cosmética") para la gestión del cumplimiento no exime "automáticamente" a los gestores de la organización sobre dicha materia, pero constituye un indicio favorable de diligencia.
f. Creación de *protocolos y guías*[629]. Por ejemplo, piénsese en el protocolo de identificación de las *actividades vulnerables* de comisión de delitos relacionados con la protección de datos dentro de la empresa.
g. El establecimiento de un *sistema disciplinario* que sancione adecuadamente el incumplimiento de las medidas. Compliance penal y protección de datos.

5.2.Responsabilidad, protección de datos y compliance.

El órgano de administración de la empresa cliente establecerá el modelo de la organización y gestión que contendrá las medidas de control y vigilancia preventivas sobre todo en materia de *protección de datos, y* será ese *"debido control"* el que podrá *eximir* (total o parcialmente) de responsabilidad civil, administrativa o penal de los administradores, directivos o subordinados dado el caso de la empresa cliente[630].

La *responsabilidad derivada de daños por incumplimiento* de la legalidad podrá dirigirse hacia personas diferentes en la organización según se hayan producido por la falta de un modelo de vigilancia adecuado o por su operación negligente[631]. El incumplimiento en el compliance actual puede derivar (PUYOL):

[629] No obstante, hay que ser cuidadosos en no "protocolizar" en exceso, sino sólo en aquellos casos en los que existan implicaciones relevantes desde la perspectiva de protección de datos personales.
[630] Los requisitos generales para esa exención serán entre otros: existencia figuras DPO-CCO; existencia de mapa de riesgos en protección de datos; protocolos no excesivamente rígidos; canal de denuncias ("whisteblowing"). Y los requisitos específicos podría ser, por ejemplo:

- Análisis de tratamientos de datos personales por cada departamento de la empresa.
- Mapa global internacional de tratamientos de datos personales en cada empresa del grupo empresarial.
- Tabla de comprobación ("benchmarking") o "chekclist del cumplimiento.
- Tabla con los plazos de conservación de datos.
- Plan de formación continua al personal.
- Sistema disciplinario interno corporativo.

[631] Según la Sentencia del Tribunal de Milán de 13 de febrero de 2008 (sección VIII de lo Civil. Stc N. 1774), la sociedad fue sometida a investigación al no disponer de un adecuado modelo organizativo y de

"a). **El aumento de la probabilidad de sanción ante las autoridades en general,** y especialmente las de protección de datos y de consumo al incrementar el número de afectados, al exponerse a jurisdicciones y leyes ajenas a su propio lugar de sede del negocio.

b). **La pérdida económica por la disminución exponencial e incontrolable** del número de potenciales clientes o consumidores y la posible pérdida de los existentes al tener constancia de su reputación digital.

c). **La falta de competitividad** para poder acudir prácticamente a cualquier licitación de naturaleza pública o privada".

d). **La pérdida reputacional"**. Es el caso de la empresa Lidl[632] y el escándalo mediático causado por la vigilancia intrusiva a sus empleados que fue sancionada con 1,5 millones de euros.

En todo caso convendría tener en cuenta los tipos de contextos o ámbitos del compliance donde se ven afectos programas de compliance de delitos relacionados con la protección de datos personales:

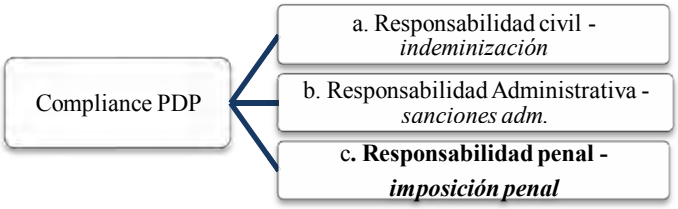


Tabla 36. Posibles tipos de responsablidad derivados de Compliace de Protección de datos personales.

Para continuar con el estudio de esta materia, convendría profundizar en la *"responsabilidad penal"* (aptdo. c) en el marco del *corporate compliance* para analizar así, el contexto en el que se desarrolla, su evolución, preceptos jurídicos, ámbito subjetivo y de esta manera, deslumbrar en qué manera afecta a las personas jurídicas u organizaciones empresariales. En la actualidad, como venimos manteniendo, la sintonía

gestión de acuerdo con la ley italiana concluyéndose una sanción de 64.000 euros como indemnización por los daños causados a la empresa.

[632] EFE (11 de septiembre 2008). Alemania multa con 1,5 millones de euros a Lidl por espiar a su empleados. *El País Economía.* Recuperado de https://elpais.com/economia/2008/09/11/actualidad/1221118375_850215.html

ética empresarial se ha vinculado estrechamente con el propio *modelo de prevención penal.* El legislador optó por atribuir responsabilidad penal a las personas jurídicas por delitos que pudieran realizar en su nombre y provechos y fueran cometidos a través de los representantes legales y administradores de derecho o de hecho (art. 31 bis 1 ab initio Código Penal). Es de señalar que el legislador no limitó el ámbito de aplicación de la jurisdicción penal a las empresas, sino que lo hizo extensible a aquellos entes que adquieren personalidad jurídica, piénsese en la fundaciones y las asociaciones que pueden dar ayuda a la comisión delictiva o reciben beneficios del delito. En definitiva, se trata de una nueva regulación que determina que la responsabilidad de la persona jurídica va a ser directa con una imputación individualizada a través de un procedimiento abreviado, lo que se traducirá en la brevedad del proceso (y del cobro de la indemnización civil)[633].

Respecto al *ámbito subjetivo*, tal y como señala José Portal (2010), "el legislador crea un sistema vicarial, *vicarious liability* puesto que la persona jurídica también responde, directamente, por no ejercitar el debido control (…)"[634] [635].

Respecto al *ámbito objetivo*, conviene señalar los siguientes aspectos:

i. La responsabilidad civil (aptdo b.) en el marco de compliance.

Tal y como señala *José Portal*, "el patrimonio autónomo que ha conseguido se encontrará afecto a la pena de multa que se le pueda imponer y, a su vez, a sufragar la responsabilidad civil *ex delicto* solidariamente con las personas físicas que fueran

[633] En otro orden de cosas, hay que tener en cuenta que las decisiones de la persona jurídica o del juzgador durante el proceso pueden "repercutir" a los stakeholders (acreedores, trabajadores, clientes o usuarios, etc..) y que serán conocedores del estado al final del proceso.

[634] Portal Manrubia, J.(2010) Publicación: *Revista Aranzadi Doctrinal* núm. 6/2010 parte Estudios. Editorial Aranzadi, S.A.U., Cizur Menor.

[635] Esto significa que la responsabilidad penal del ente jurídico puede derivarse ante la ausencia de una especie *"due diligence"* de los órganos de dirección ante el cumplimiento de la normativa sectorial en materia de protección de datos que hemos ido hablando a lo largo de estos capítulos. Esta falta de control hace que los trabajadores o subordinados ejecuten una acción punible "en nombre y beneficio" de la organización empresarial. Por tanto, la organización podría responder por la comisión de un hecho ilícito ejecutado por alguno de sus empleados siempre que la acción se cometa en provecho de la misma. En otro orden de cosas, hay que hacer una precisión: el legislador excluye la responsabilidad penal del Estado, de las Administraciones Públicas, territoriales e institucionales, y de aquellas que ejerzan potestades públicas de soberanía, administrativas o sociedades mercantiles estatales que ejecuten políticas públicas o presten servicios de interés económico general (art. 31 bis 5 CP), por lo que, proveedores de salud públicos no podrán ser sujetos de responsabilidad penal.

condenadas por los mismos (art. 116.3 del CP)" .También señala algo interesante y que venimos diciendo: "dichas consecuencias de carácter económico pueden comprometer la viabilidad del ente, así como perjudicar a terceros, stakeholders , v. gr. sus trabajadores".

ii. *Atenuaciones por actuaciones postdelictivas en el marco de compliance.*

Según este autor, "el legislador prevé que para la imposición de la pena se tengan en consideración una sucesión de *actuaciones postdelictivas*[636] que permiten atenuarla sin que, en ningún momento, lleguen a eximirla (art. 31 bis 4 CP)". Por tanto, entendemos que, haber integrado *medidas de control eficaces en su estructura* o programas de compliance para prevenir y descubrir los delitos que pudieran cometerse (art. 31 bis 4 d) podrían atenuar la pena. En todo caso y extendiendo este precepto al ámbito de protección de datos, hay que tener en cuenta que si el objeto de *compliance penal* es obtener ciertas *"evidencias"* ; las empresas responsables y encargadas del tratamiento deberán demostrar que han utilizado las medidas correspondientes (organizativas, técnicas y garantías suficientes)[637] en materia de protección de datos. En mi humilde opinión, se echa de menos que el legislador no haya aprovechado la oportunidad que brinda toda nueva normativa para incorporar algún mecanismo que pudiera "premiar" a los proveedores tecnológicos más transparentes y diligentes y "sancionar" a aquellos que incumplen.

iii. La revelación de secretos informáticos (art. 197.2 CP) y el acceso informático ilícito (art. 197.1 CP) en relación con el art. 31 bis.

[636] "Dichas circunstancias consisten en; haber procedido la persona jurídica a la *confesión* de la comisión del hecho punible con anterioridad a conocer que el proceso penal se dirige contra la misma (art. 31 bis 4 a) CP); *cooperar en todo momento con la investigación*, aportando fuentes de prueba desconocidas que ayuden a esclarecer la responsabilidad penal de acorde con los hechos investigados (art. 31 bis 4 b); proceder a la reparación o disminución del daño causado por el delito con anterioridad al juicio oral (art. 31 bis 4 c); y, por último, haber integrado *medidas de control eficaces en su estructura*, compliance programs, con el fin de prevenir y descubrir los delitos que pudieran cometerse (art. 31 bis 4 d)".

[637] Por ejemplo, medidas como que se han adoptados políticas internas y se han aplicado las medidas correspondientes de protección de datos desde el *diseño y el defecto*, que su encargado se ha adherido a un *código de conducta o certificaciones, q*ue tanto el cliente y responsable como el encargado deberán demostrar el *registro* de las posibles incidencias (ej.: fugas de información) las cuales deberán ser informadas a la autoridad de control (AEPD) y que ha realizado una *evaluación de impacto* (riesgo y el origen, ámbito del tratamiento y orígenes del tratamiento) dado el carácter de categoría de datos especiales de los datos y que se ha designado DPO.

Los delitos relacionados con este precepto estarán vinculados estrechamente a la vulneración del derecho fundamental de protección de datos de las personas físicas.

Respecto al delito de "revelación de secretos informáticos", el abogado y profesor de Derecho Penal y Compliance, Francisco Bonatti[638], diferencia acertadamente tres comportamientos en este precepto:

a. *"Apoderarse, utilizar o modificar*[639] *sin autorización datos reservados* de carácter personal o familiar que se hallen registrados[640] en ficheros o soportes informáticos, electrónicos o telemáticos o en cualquier otro tipo de *archivo público* (caso Boehringuer) o privado"[641].

> Por ejemplo, piénsese en hechos delictivos de empleados públicos (informáticos) de un hospital de Lleida que acceden a la intranet del hospital pudiendo acceder a contraseñas, geolocalización, DNI, etc. y al historial médico electrónico de otras personas motivadas por un precio o compensación económica (espionaje)[642].

---

[638] Bonatti, F. *Delitos contra la intimidad - Protección de los datos personales y familiares reservados. El "espionaje" personal y corporativo.* Recuperado de https://www.bonattipenal.com/delitos-contra-la-intimidad-proteccion-de-los-datos-personales-y-familiares-reservados-el-espionaje-personal-y-corporativo/

[639] Vid. Sentencia Penal Nº 892/2015, Audiencia Provincial de Barcelona, Sección 7, Rec 23/2015 de 26 de Noviembre de 2015). (Señala que "Modificar es alterar los mismos, tanto si se trata de mejorar como de perjudicar la situación del sujeto al que afectan. Las conductas tienen que producirse sin estar autorizado para acceder, manipular o modificar el banco de datos y realizarse en perjuicio de tercero, tercero que puede ser distinto al titular de los datos produciéndose una triple implicación de sujetos (sujeto activo, titular de lo datos y eventual perjudicado) que responde, a la idea de que el titular de los datos no puede ser sujeto activo del delito porque él es el sujeto pasivo, dado que lo tutelado es su intimidad".)

[640] *Ibídem.* (Señalaba que "en el sentido del art. 197.2 debe exigirse que se trate de un conjunto organizado de información relativa a una generalidad de personas. Dado el carácter reservado de los datos, los ficheros o registros han de ser de acceso y utilización limitada a personas concretas y con finalidades especificas, siendo indiferente, su naturaleza: personal, académica o laboral, medica, económica, etc... Se trata, en realidad de informaciones de carácter personal relacionadas más con la privacidad que con la intimidad. Las conductas van dirigidas a datos que se hallen registrados, es decir a bancos de datos preexistentes, entendiéndose por la doctrina que no es típica la creación clandestina de bancos de datos, que queda en el ámbito administrativo sancionador").

[641] Vid. STS Sentencia Penal Nº 144/2018, Audiencia Provincial de Lleida, Sección 1, Rec 233/2017 de 03 de Abril de 2018. (Señalaba que "Se trataría del perjuicio se realiza cuando se apodera, utiliza, modifica o accede a un dato protegido con la intención de que su contenido salga del ámbito de privacidad en el que se incluyó en una base de datos, archivo, etc., especialmente protegido, porque no es custodiado por su titular sino por titulares de las bases con especiales exigencias de conductas de protección". El tipo penal del art. 197.2 "exige que la conducta se lleve a cabo en *perjuicio de tercero*, *aunque no haya un ánimo* específico de perjudicar, pues basta con que la acción se realice con la finalidad dicha, sin que resulte necesario para la consumación la producción del resultado lesivo").

642 No obstante, en sentencias como la STS 532/2015, de 23 de septiembre, se refiere a un perjuicio que perjudica a su titular por el mero "acceso" a los datos sensibles (es decir, sin necesidad de un móvil económico). "Mientras que en los datos 'no sensibles', no es que no tengan virtualidad lesiva suficiente para provocar o producir el perjuicio, sino que debería acreditarse su efectiva concurrencia." (Sentencia Penal Nº 892/2015, Audiencia Provincial de Barcelona, Sección 7, Rec 23/2015 de 26 de Noviembre de 2015).

Sin ir más lejos, en España, hace un par de años, ya la Fiscalía[643] del TSJ de Andalucía y la AEPD investigaba el presunto caso de revelación de secretos y derechos fundamentales a la intimidad de datos personales y de salud de la farmacéutica alemana *Boehringuer* que afectan a numerosos pacientes y fueron denunciados por la **Asociación Defensor del Paciente.** Un ex trabajador de la empresas farmacéutica, enviaba documentación para ejercer su labor de lobby[644] favorable a los fármacos de la empresa farmacéutica, hechos que pueden ser constitutivos de diversos delitos y prácticas irregulares por *parte de la empresa y de funcionarios de los* **Sistemas Sanitarios de Andalucía y Extremadura.** Según el periódico nueva tribuna[645], los presuntos hechos eran **"**descubrimiento y revelación de secretos de Salud sin consentimiento de los propietarios de ficheros, con presunta coacción y abuso confianza a funcionario público como facilitador. La empresa como persona Jurídica sería además responsable por existir conocimiento de los hechos por parte de Directivos y Administradores de la misma. La empresa alemana habría recabado documentación médica con datos de salud y de gestión sanitaria, documentos internos de gestión clínica, sin consentimiento de los propietarios de los ficheros y con presunta coacción y abuso de confianza a funcionario público como facilitador. Asimismo, funcionarios y personal de los Servicios Sanitarios Públicos de la Comunidad Autónoma de Andalucía y Extremadura estarían implicados".

Según las pruebas aportadas en la denuncia, "se utilizaron técnicas de imagen, acceso a emails internos, pantallazos de sistemas informáticos de gestión sanitaria, obteniéndose documentos internos de salud, de los servicios autonómicos de salud de Andalucía y Extremadura" (Asociación defensor del paciente).

Concretamente, por ejemplo, podemos señalamos ejemplos de estas técnicas según los periodistas:

> "-Extracción ilícita y posterior difusión de pantallazos de terminales informáticos *(ver imagen inferior)* extraídos de los programas informáticos de gestión clínica de los Servicios Andaluz y Extremeño de Salud, conteniendo nombre del paciente, patología que padece, medicación prescrita, nombre del médico prescriptor, etc. Según El Confidencial[646], se difundió la imagen de una pantalla de ordenador en la que se mostraba la prescripción a un paciente del **fármaco "Striverdi" (ver imagen inferior)** a través del sistema Diraya, que es el que se utiliza en el Sistema Sanitario Público de Andalucía como soporte de la **historia clínica electrónica.**

[643] Ver Decreto de Apertura (27 de marzo 2017) de Fiscalía Superior de la Comunidad Autónoma de Andalucía . Diligencias de Investigación Penal n.8/2017 (NGF 217/17). Recuperado de https://www.elconfidencialdigital.com/media/elconfidencialdigital/files/2017/04/08/ECDFIL20170408_0001.pdf

[644] Toda esta información filtrada serviría a Boehringer para **ejercer presiones** contrarias a los criterios de eficiencia y gestión clínica de los profesionales sanitarios. Se podría **interferir en las políticas sanitarias** sobre el uso de medicamentos, eficiencia y sostenibilidad del sistema sanitario, autorización de visados de inspección médica y hasta en la celebración de subastas de fármacos.

[645] NuevaTribina (11 de abril de 2017). Boeringher, nuevamente en la picota. Recuperado de https://www.nuevatribuna.es/articulo/sanidad/boehringer-nuevamente-picota/20170411175606138694.amp.html

[646] Decreto de Apertura (27 de marzo 2017) de Fiscalía Superior de la Comunidad Autónoma de Andalucía. Diligencias de Investigación Penal n.8/2017 (NGF 217/17). Recuperado de https://www.elconfidencialdigital.com/media/elconfidencialdigital/files/2017/04/08/ECDFIL20170408_0001.pdf

Desde mi opinión, el interés comercial y económico podría estar detrás de esto. Se trata de un medicamento que está siendo probado en ensayos clínicos[647] para personas con asmas (más de 3 millones en España, según Novartis) . Y es que, ¿porqué se realizaron estas extracciones de información sensible de los ciudadanos (datos personales tachados, en negro en la imagen , por ej. hombre, 72 años, etc.,)? ¿ el móvil económico de la farmaceutica está detrás de todo ello? ¿o son otros intereses?

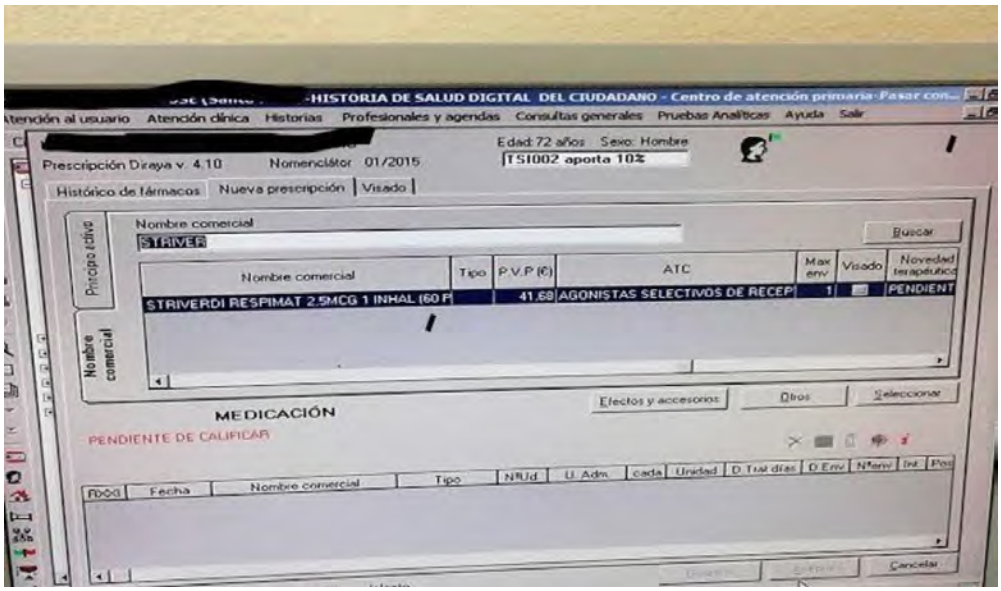


Imagen 65. Pantallazo prueba documental aportado en el procedimiento Boehringher-Servicios de Salud Andaluz y Extremeño.

-Extracción ilícita y posterior difusión interna en la Empresa de Recetas con nombres de pacientes, DNI, medicación prescrita, etc., facilitadas por funcionarios públicos (coacción y abuso confianza).

-Extracción ilícita y posterior difusión en BIESA de envíos internos de *algoritmos de manejo de fármacos* recomendados por distritos sanitarios de primaria, en base a criterios de seguridad y eficiencia, que envían las Áreas Sanitarias de Servicios Autonómicos de Salud a toda la organización de profesionales sanitarios.

-Extracción ilícita y posterior *difusión de emails internos del SAS*, emitidos por Farmacéuticos/as de Atención Primaria a todo el colectivo de centros de salud":

Se señaló, además, que la empresa presionó al trabajador a la entrega de las pruebas documentales que recibió en su mail corporativo, procedentes de la propia empresa a pesar de tener los numerosos datos personales, negándose el trabajador para no incumplir su obligación de confidencialidad, situación que le costó la suspensión de 45 días de empleo y sueldo. Me parece un caso bastante significativo que recoge hechos graves donde se vulneran los derechos fundamentales de las personas (pacientes, trabajadores) y

[647] Ver https://es.wikipedia.org/wiki/Olodaterol

que pueden ser susceptibles de una clara responsabilidad penal recogida en los preceptos penales que hemos mencionado (archivos públicos donde la A.P. es responsable del fichero). Es de señalar la dificultad que he tenido en encontrar pronunciamiento alguno por parte de la AEPD quien iba a investigar de oficio este caso en el 2018 respecto a la responsabilidad del Servicio de Salud Andaluz[648] en estos presuntos hechos, o pronunciamiento alguno por parte del gobierno Andaluz.

b. "Acceder sin autorización por cualquier medio a los mismos".

Por ejemplo, piénsese en un hacker que tuviera el encargo de acceder al sistema informático de un hospital y obtener los datos[649]".

c. "Alterarlos o utilizarlos en perjuicio del titular de los datos o de un tercero".

Por ejemplo, piénsese en quien, sin tener nada que ver con la trama que obtiene los datos, llegan a su poder y los utiliza, por ejemplo haciéndolos públicos para dañar a la persona.

Este tipo de hechos delictivos no sería el más frecuente por la naturaleza del contexto, en todo caso motivado por el componente económico.

Respecto del delito de "acceso informático ilícito" (Art. 197.1 CP) se trata de una infracción menos grave que la de revelación de secretos informáticos y no tiene porqué motivarse por la intención de descubrir secretos personales. El hecho delictivo se realiza accediendo a datos o archivos del ordenador del titular de los mismos. No obstante, no tienen porque ser únicamente datos "personales" identificables a una persona. Por tanto, la intención del legislador no era proteger esta categoría de datos sino el hecho de "saltarse" las medidas de seguridad y acceder a los registros informáticos de una persona.

Destacar algo muy importante: a diferencia de la revelación de secretos informáticos es imprescindible para acceder a los datos la vulneración de las medidas de seguridad. Como señala Bonati "la ley no castiga el acceso a los datos que el propio usuario no protege".

iv. Art. 197 CP bis (en relación con el art. 31 bis)

[648] Según ha podido confirmar *El Confidencial Digital* por fuentes conocedoras del caso, la filtración incluye también un listado con los nombres de los vocales de todas las Comisiones de Farmacia de los hospitales Virgen del Rocío y de la Macarena, en Sevilla.

[649] Vid. https://cuadernosdeseguridad.com/2018/04/alertan-del-incremento-de-ciberataques-a-equipos-medicos-en-2018/

Convendría destacar por la novedad que supone el art. 197 bis que extiende la protección penal contra quienes por cualquier medio o procedimiento, vulnera las medidas de seguridad establecidas para impedirlo y sin estar debidamente autorizado, facilite a otro el acceso al conjunto o a una parte de un sistema de información.

v. Art. 197 quienquies (en relación con el art. 31 bis)

Contempla el caso de que sea una persona jurídica (organización empresarial) sea responsable de los delitos 197, 197 bis, 197 ter, que se refiere a la producción, adquisición o distribución a terceros de programas informáticos, concebidos para cometer los delitos anteriores, o una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad, o a una parte, de un sistema de información. En este caso a la empresa se le pondrá una pena de 6 meses a dos años y, atendidas las reglas establecidas en el art 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33, entre las que se encuentran la disolución de la persona jurídica, la suspensión de sus actividades por un plazo que no podrá exceder de 5 años, la clausura de sus locales etc.

5.3.Canales de denuncia ("*whistleblowing*")

Se tratan de una herramienta adecuada y eficaz para la detección de ilícitos cometidos para ser utilizada no sólo por empleados sino por terceros, como por ejemplo, los clientes o proveedores tecnológicos/subcontratistas. Si hablamos de *whistleblowing* no podemos dejar de lado el caso grave de *Boehringer Ingelheim* citado anteriormente. Como decíamos, esta farmacéutica fue investigada por Fiscalía ante presuntos hechos penales por violación del derecho fundamental de intimidad y de protección de datos de pacientes y trabajadores funcionarios (art. 262 Lecr[650]). Es una situación un tanto

[650] "Los que por razón de sus cargos, profesiones u oficios tuvieren noticia de algún delito público, estarán obligados a denunciarlo inmediatamente al Ministerio Fiscal, al Tribunal competente, al Juez de instrucción y, en su defecto, al municipal o al funcionario de policía más próximo al sitio, si se tratare de un delito flagrante. Los que no cumpliesen esta obligación incurrirán en la multa señalada en el artículo 259, que se impondrá disciplinariamente. Si la omisión en dar parte fuere de un Profesor en Medicina, Cirugía o Farmacia y tuviesen relación con el ejercicio de sus actividades profesionales, la multa no podrá ser inferior a 125 pesetas, ni superior a 250.Si el que hubiese incurrido en la omisión fuere empleado público, se pondrán además en conocimiento de su superior inmediato para los efectos a que hubiere lugar en el orden administrativo. Lo dispuesto en este artículo se entiende cuando la omisión no produjere responsabilidad con arreglo a las Leyes".

delicada pues como al parecer según la Asociación "el defensor del paciente"[651], "debido al acoso y menoscabo a su dignidad y salud laboral, que el trabajador sufrió en este conflicto, actualmente sufre una incapacidad laboral permanente total con diagnostico de "trastorno adaptativo" a causa de verse involucrado el trabajador en este conflicto supuestamente penal, ajeno a su responsabilidad"[652].

En otro orden de cosas, la norma ISO 19600:2014, sobre Sistemas de Gestión de Compliance, en la cláusula 10.1.2 señala la obligatoriedad de esta herramienta:

> "(…) Un sistema de gestión de Compliance eficaz debería incluir un *mecanismo* para que los empleados de la organización y/u otras personas *informen* sobre *malas prácticas reales o sospechosas*, o sobre violaciones de las obligaciones de Compliance de la organización, de forma confidencial y sin temor a represalias".

También, la Directiva[653] (aprobada en el mes de abril de 2019) en protección de las personas que denuncian las infracciones del Derecho de la Unión, donde una de las principales innovaciones introducidas (Art. 4 del Capítulo II) introduce la obligación de establecer canales o sistemas de denuncia internos. La obligación alcanza a las siguientes entidades: i) empresas privadas que cuenten con una plantilla de, al menos, cincuenta empleados; ii) empresas privadas con una cifra de negocio o un balance anual de al menos diez millones de euros; iii) empresas privadas que operen en el ámbito de los servicios financieros o se encuentren afectadas por la regulación relativa a la prevención de blanqueo de capitales y financiación del terrorismo; iv) entidades de la administración estatal; v) entidades de la administración regional y sus departamentos;

---

[651] Vid. https://interprofesionalgranada.files.wordpress.com/2017/09/comunicado-a-la-presidencia-y-consejeria-de-salud-de-la-junta-de-andalucia.pdf

[652] Estos hechos estaban relacionados con "el acceso y obtención ilícita a datos e información de sistemas informáticos de gestión clínica , propiedad de los Servicios Autonómicos de Salud de Andalucía y Extremadura. Información que contiene numerosos datos personales , de salud, de Gestión Clínica, Farmacéutica e Inspección Médica". Este tipo de situaciones requerirán de respuestas y protocolos claros de cumplimiento normativo por parte de todos los actores intervinientes, incluida la propia Administración Pública.

[653] Comisión Europea. Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la proteccion de las personas que informen sobre infracciones del Derecho de la Unión. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018PC0218&from=ES y https://confilegal.com/20190417-la-union-europea-aprueba-la-directiva-de-proteccion-a-los-denunciantes-de-corrupcion-o-whistleblowers/

vi) entidades de municipios de, al menos, diez mil habitantes; vii) otras entidades reguladas por Derecho Público[654].

A su vez, *la Circular 1/2016 de la Fiscalía General del Estado* entiende que la existencia de unos canales internos de denuncia conforma uno de los elementos de mayor relevancia en los sistemas de compliance. El texto del Código Penal reconoce en su apartado 4 del Art. 31 bis la imposición de la obligación de informar internamente posibles riesgos e incumplimientos. Y no sólo eso, también el RGPD prevé también líneas de comunicación internas directas en el art. 36.2 ("el delegado de protección de datos informará directamente a la dirección del responsable o del encargado del tratamiento"), sistema de comunicación que podría ser reforzado con un sistema de whistleblowing para comunicar esos riesgos de forma "confidencial". El escenario ideal sería unificar ambos canales de denuncia (penales e infracciones administrativas).

Ahora bien, se me ocurren varios interrogantes:

- ¿Cómo puede participar el DPO en las investigaciones internas corporativas? El mayor problema lo encuentro posiblemente en diferenciar los casos de uso ordinario de datos de los de usos motivados por comisión de un delito. En todo caso, resultará de especial importancia la preservación de la cadena de custodia de las evidencias digitales para garantizar la trazabilidad en la investigación interna.
- ¿Es posible sancionar disciplinariamente al trabajador que no cumple con su obligación de informar sobre las conductas ilícitas que se produzcan en la organización? Habría de atenderse al caso concreto y en función de factores como el cargo del empleado y el tipo de incumplimientos que se están produciendo. No sería la misma situación para un trabajador que tenga funciones de control y de transparencia (ej. CCO) como un trabajador que sus funciones se alejan de ese control ético. Tampoco será igual el incumplimiento grave dentro del programa de

[654] Y en todo caso, los procedimientos de denuncia y tramitación de denuncias deberán incluir lo siguiente: a) cauces para recibir denuncias que estén diseñados, establecidos y gestionados de tal forma que se garantice la confidencialidad de la identidad del informante y se impida el acceso al personal no autorizado; b) *designación de la persona* o del servicio competente para tramitar las denuncias; c) tramitación diligente de las denuncias por la persona o el servicio competentes; d) plazo razonable, no superior a tres meses tras la presentación de la denuncia, para comunicar al informante el curso dado a la misma;e)información clara y fácilmente accesible sobre los procedimientos y sobre cómo y en qué condiciones pueden presentarse denuncias ante las autoridades competentes de conformidad con el artículo 13, apartado 2, y, en su caso, ante los órganos y organismos de la Unión.

prevención de delitos (compliance program) que una irregularidad sin perjuicio económico para la empresa.

En conclusión, la obligatoriedad de los canales de denuncias aparecen como novedad y supone un giro radical en el funcionamiento interno de las empresas que hasta ahora se percibía como simple recomendación. No obstante, "los derechos fundamentales constituyen pues un límite infranqueable a la actividad de compliance empresarial" (J. R. Agustina, 2015) [655]. Como he venido señalando reiteradamente, la tecnología blockchain y los sistemas DLT puede resultar de gran utilidad para posibilitar dicha trazabilidad en el contexto de compliance (control horario laboral, cumplimiento PRL); ¿por qué no podría servir para acreditar el cumplimiento en protección de datos? En el capítulo correspondiente hablaremos de soluciones blockchain que ya son utilizadas para ello.

6. RESPONSABILIDAD SOCIAL EMPRESARIAL O CORPORATIVA.

En la introducción de la norma ISO 19600: 2014 ya se decía que "el *compliance* también contribuye al comportamiento socialmente responsable de las organizaciones". No obstante, se puede caer en el error de no diferenciar claramente los conceptos entre "ética empresarial" y "RSE" ya que la primera se refiere a comportamientos o actuaciones "correctos" y la segunda se refiere más bien al conjunto de actividad que se realiza para controlar su impacto.

Ética Empresarial	*RSE*
Ref. a comportamientos o actuaciones considerados como *correctos* dentro de la empresa	Ref. al conjunto de actividades que esta realiza para *controlar su impacto.*
Condicionados por *stakeholders*	Puede haber código ético o no

Tabla 37. Diferencias entre ética empresarial y RSE.

[655] ALCACER GUIRAO,R., "Cumplimiento penal por la persona jurídica y derechos fundamentales: la intimidad como límite a la vigilancia empresarial", *Diario La Ley* , Núm. 8053, Sección Doctrina, 2 Abr. 2013, Año XXXIV, Ref.D-118, LA LEY 1685/2013 . En AGUSTINA, J.R. "el DPO en el marco de la responsabilidad penal". Recuperado de https://www.academia.edu/11420153/El_Data_Protection_Officer_en_el_marco_de_la_responsabilidad_penal_de_las_personas_jur%C3%ADdicas_Consideraciones_a_la_luz_del_nuevo_Reglamento_Europeo_en_materia_de_protecci%C3%B3n_de_datos

Quisiera hacer una aclaración previa; cuando se habla de RSE no sólo se la puede relacionar con el sector privado sino también con el sector público ("responsabilidad social institucional o pública"), que no es lo mismo que "compliance público"[656]. Como veremos "responsabilidad social corporativa" y *"compliance"* o cumplimiento normativo son conceptos diferentes.

El Foro de Expertos en RSE del Ministerio de Trabajo[657] estableció la siguiente definición:

> "L**a RSE es** el *cumplimiento estricto* de las obligaciones legales vigentes, la *integración voluntaria* por parte de la empresa, en su gobierno y gestión, en su estrategia, políticas y procedimientos, de las preocupaciones sociales, laborales, medioambientales y de *respeto a los derechos humanos* que surgen de la relación y el diálogo transparentes con sus grupos de interés, responsabilizándose así de las consecuencias y de los impactos que se derivan de sus acciones".

De esta definición me gustaría sacar las siguientes conclusiones; (i) se trata de un cumplimiento estricto (o más bien de su voluntariedad o predisposición) (ii) ser responsable social implica ser diligente ante exigencias reguladoras (autorreguladoras y heterorreguladoras) en nuestra materia; (iii) se incluye el respeto a los derechos humanos como objetivo, en el cual se incluye el derecho fundamental de la protección de datos personales[658]; (iv) sucede en el contexto del diálogo de diferentes *stakeholders*.

En cualquier caso, "la transparencia es un principio esencial que debe presidir las relaciones entre las partes, especialmente en los casos en que el proveedor de servicios ocupa una posición preeminente sobre los clientes"[659] [660]

---

[656] Campos, C. (2018). *Compliance en el Sector Público ¿necesidad o virtud?*. Recuperado de http://concepcioncampos.org/compliance-en-el-sector-publico-necesidad-o-virtud/ (La autora utiliza el concepto del "compliance público").

[657] http://www.mitramiss.gob.es/es/sec_trabajo/autonomos/economia-soc/RespoSocEmpresas/foro_expertos/index.htm

[658] En este sentido, ya la declaración Universal de los Derechos Humanos establecía en relación con la privacidad que "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su correspondencia, ni de ataques a su honra o su reputación".

[659] En palabras de Jorge Salgueiro (presidente de la comisión compliance de EuroCloud): "es preferible que las patronales actúen con responsabilidad social corporativa elaborando códigos de buenas prácticas y de conducta". Ver en http://www.diarioabierto.es/291570/jorge-salgueiro-la-autorregulacion-es-necesaria-hasta-que-los-mercados-maduren

[660] No obstante, se debe tener en cuenta que se trata de un término que engloba y alcanza a los propios clientes de servicios tecnológicos en tanto que su decisión y relación con los proveedores tecnológicos puede tener impacto en los derechos y libertades de las personas, más concretamente, en el derecho fundamental de la protección de datos personales. La RSE tiene que ver con la gestión ética y con el compromiso de actuar responsablemente. Proveedores y clientes deberán tener en cuenta en su proceso

A continuación, podemos perfilar de alguna manera los intervinientes o actores que participan en la RSE -sea empresarial o sea institucional- orientada a un esquema tecnológico:

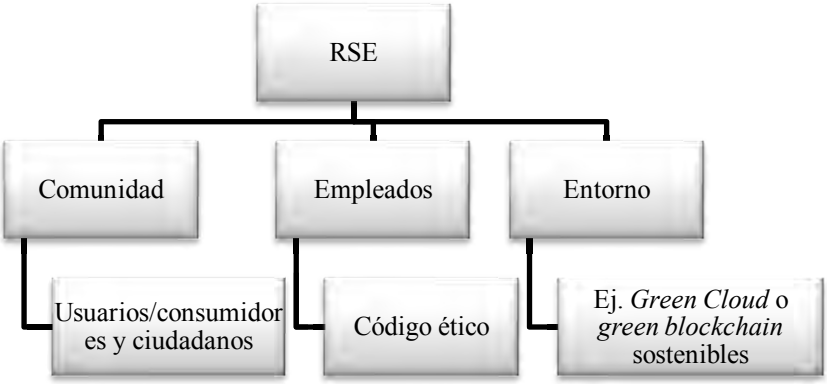


Tabla 38. Esquema de RSE y elementos. Fuente propia.

Como se puede ver, la RSE se podría extender a tres ámbitos:

i. *A la comunidad* donde se incluyen a los usuarios, consumidores y ciudadanía como titulares de derechos y libertades. El derecho de protección de datos es un *derecho fundamental*[661] el cual reconoce la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos.

ii. *A los empleados de la organización o institución* que deberán seguir los códigos éticos y serán responsables de la adecuada utilización de los activos intangibles de la organización protegiéndolos del mal uso, sabotaje o pérdida. Éstos deberán conocer las medidas de seguridad adecuadas para proteger la confidencialidad de los datos personales y tener especial cuidado con la pérdida de control de la información de carácter personal a terceros, debiéndose asegurar de que el envío se realiza por razones legítimas de negocio y que cumple la legislación local.

---

de implantación de RSE los siguientes aspectos: 1. *Cumplimiento de la legislación y normativa.* Tener RSE en una organización o institución implica en cumplir "más allá" de lo que la propia legislación establece. 2. *Política de Gestión Ética y Responsabilidad Social***.** La política o el plan de RSE deberá ser visible públicamente y firmada por el máximo responsable y contendrá objetivos medibles, comparables y verificables pudiéndose revisar anualmente. Además, en el c*ódigo de conducta* se definirá el canal para resolver dudas, sugerencias o denuncias y medidas sancionadoras en caso de incumplimiento. 3. *Comité de Gestión Ética y Responsabilidad Social*. Podrá nombrarse por el CEO y estará formado por áreas diferentes de gestión incorporando expertos externos incluso, los cuales se reunirán al menos una vez semestralmente. Sus tareas serán (i) buscar los riesgos legales que puedan afectar a la organización; (ii) supervisar los planes asegurándose de que se cumplen las buenas prácticas y el código ético; (iii) establecer un sistema para dialogar con los grupos de interés (quejas, sugerencias abiertas a los clientes) y se nombrará a un responsable de RSE; (iv) hacer seguimiento de evaluación y mejora continua, revisándose la política, el código de conducta, el plan, los objetivos, el modelo de diálogo con los grupos de interés, los informes de auditoría y las acciones correctivas y preventivas puestas en marcha.

[661] Ver definición de protección de datos como derecho fundamental https://www.agpd.es/portalwebAGPD/common/FOLLETO.pdf

iii. *Al entorno.* Se refiere al uso eficiente de los recursos materiales minimizando el impacto ambiental, maximizando su viabilidad económica y asegurando los deberes sociales. El mejor uso de la tecnología incluye la optimización en el uso de la energía, el uso de materiales menos contaminantes, la reducción sustancial del espacio físico y la optimización en la gestión de los recursos[662]. Por ejemplo, se refiere a lo que se viene denominando *"eco o green cloud"* [663] o "eco o *green blockchain mining"*. El gasto de energía en enfriamiento llega a representar una cantidad equivalente a lo consumido directamente por los servidores tanto en cloud como en blockchain.

La RSE no se trata de un control unilateral sino una participación de todas las partes implicadas: cliente, proveedor y subproveedores en el contexto empresarial o institucional. Si trasladamos todo ello al ámbito de protección de datos los participantes serían:

i. *La empresa o institución cliente "responsable".* La adaptación de las empresas proveedoras a los estándares solicitados por las empresas clientes debe ser fruto de un proceso de diálogo y de trabajo conjunto. La gestión de riesgos en materia de protección de datos de las grandes organizaciones multinacionales requieren de un nuevo paradigma de cooperación y coordinación entre estas ellas. Los clientes con presencia dominante en la cadena de valor podrán ejercer un *papel de liderazgo* en la promoción de la RSE, proporcionando apoyo a proveedores que la implanten el estilo, en forma de incentivos, formación o tutelaje en materia de protección de datos.

ii. *La empresa o institución proveedora "responsable".* Desde la dirección de la empresa proveedora se deberá trabajar la RSE frente a los subcontratistas o subproveedores. Éstos últimos deberán adherirse a su código ético de conducta y cumplir con los requisitos solicitados necesarios ya que es el proveedor quien tendrá que vigilar el cumplimiento de éstos y responda frente a los clientes[664].

iii. *La cadena de suministro "responsable".* La puesta en práctica no será nada fácil pero lo determinante en estos casos es que tanto cliente como proveedor no pierdan de vista los siguientes 3 elementos: Involucración conjunta, diálogo con grupos de interés y evitar a empresas con málas prácticas.

---

[662] Unión Europea. Programa Energía Inteligente para Europa IT e Infraestructura energéticamente eficiente para centro de datos y sala de servidores PrimeEnergyIT Project, Viena, 2011, p.3, p.52

[663] Ver https://es.wikipedia.org/wiki/Green_computing

[664] Microsoft reconoce en su apartado de RSE que ha avanzado en varios frentes como al convertirse en el primer proveedor de la nube principal objeto de verificación independiente para satisfacer primera norma internacional del mundo para la nube privada (llamada ISO / IEC 27018) pero no olvidemos que *no existe "compromiso"* de cumplirlo permanentemente, ni pretenden adquirir ningún tipo de responsabilidad o sanción. He aquí, la importancia de los códigos de conducta con compensación o penalización ante incumplimiento de sus cláusulas.

A continuación, señalo algunas cuestiones generales a tener en cuenta en el futuro de la RSE y la cadena de suministro :

1. *El sector privado tecnológico* apoyará la implementación de medidas y la cultura de la transparencia y ética intercambiando buenas prácticas (también entre los entes de la cadena de suministro. No obstante, las organizaciones tecnológicas gigantes presionarán a los gobiernos para obtener los mejores intereses para ellas mismas[665].
2. *Las Administraciones Públicas.* Se encargarán de la presión reguladora sensibilizando a organizaciones empresariales y a las pyme. Las autoridades de control serán esenciales.
3. La *sociedad civil.* Se empoderará tecnológicamente y "juzgará" la imagen de las organizaciones posicionando su reputación.
4. Los *stakeholders* sensibilizarán a las organizaciones con *benchmarking*, es decir, por evaluación mediante comparación con un estándar, checklist, certificación, sello o código de conducta en protección de datos.

En definitiva, invertir en responsabilidad social empresarial supone por un lado, *beneficios tangibles* como la reducción de costes, mejoras en la calidad y reducción de sanciones y costes en procedimientos judiciales o arbitrales, y por el otro lado, *beneficios intangibles* ligados a la mejora de imagen reputacional.

7. EL RÉGIMEN SANCIONADOR.

7.1.El régimen sancionador en el RGPD.

En primer lugar, me gustaría indicar algunas de las novedades más destacables que se pueden deducir tras la lectura del art. 83 y 84 del RGPD.

a. Finalidad del nuevo régimen sancionador.

El legislador, con el RGPD, pretende reforzar la protección del derecho fundamental y no quedar invulnerable en ningún Estado miembro a través de la armonización, superando la des homogeneización que permitía la antigua Directiva europea (art.24)[666]. Se prevé que las multas administrativas serán *efectivas, proporcionadas y disuasoria* (considerando 152) y se impondrán en función de las circunstancia, lo que evidencia

[665]https://www.tercerainformacion.es/articulo/internacional/2019/03/03/facebook-desarrollo-una-operacion-global-de-lobby-para-atacar-a-las-leyes-de-proteccion-de-datos

[666] En el considerando 11 del RGPD señala que la protección de datos personales en la UE deberá ser efectiva y reforzada donde los derechos y las obligaciones queden especificados, siendo los EEMM tengan poderes de supervisión y garantía para el cumplimiento recurriendo a las sanciones en caso de infracciones. Es decir, la norma europea deja margen de maniobra para que los EEMM desarrollen y la completen.

una apuesta clara por el principio de responsabilidad proactiva, de cada caso individual[667]. Según Corral (2016, 581) [668] el objetivo de esta apuesta es doble; por un lado, "*humanizar las sanciones* en supuestos en que los responsables sean personas físicas y Pymes", y por otro, "premiar la conducta responsable y vocacionalmente cumplidora de la legislación de protección de datos cuando se hubieran cometido infracciones sin intención (o a título de mera inobservancia) pero, al mismo tiempo, se haya reaccionado con diligencia para paliar sus efectos.[669]

b. Objetivo y naturaleza de las sanciones.

El RGPD establece un sistema de sanciones o actuaciones correctivas que permite un amplio margen de apreciación. Corral (2016, 574) señala que ahora con el RGPD, podrían deducirse dos tipos de sanciones. En primer lugar, "sanciones económicas (multas administrativas) para las infracciones previstas en el art. 83 que son la mayoría" donde no se dejaría margen alguno a los EEMM para regular más allá. Y en segundo lugar, las referidas al art. 84, para las infracciones no referidas en anterior artículo, es decir, para aquellos supuestos no tipificados en los apartados 4,5, y del art. 83, donde sí se dejarían un margen amplio a los EEMM para desarrollar normativa siempre respetando el principio de proporcionalidad[670].

c. Endurecimiento de las sanciones y tipificación.

Como bien es sabido, con la llegada del RGPD, el régimen sancionador *se endurece*, no solo para los responsables del tratamiento de los datos, sino también a los encargados, procediendo a incrementar las cuantías de las sanciones por incumplimiento

[667] Todo ello a título adicional o sustitutivo de las medidas contempladas en el artículo 58.2 (asesorar al responsable, emitir dictámenes, aprobar normas corporativas vinculantes, etc..) en donde se relacionan los poderes correctivos que disponen las Autoridades de Control.

[668] Corral, Alejandro, "Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad" Dtor. J.L. Piñar, 2016, en "El régimen sancionador en materia de protección de datos en el Reglamento General de la Unión Europea". Página 274.

[669] Rallo Lombarte, A., Estudios sobre la evolución del régimen sancionador en la legislación de protección de datos. *Revista de Estudios Políticos*, núm. 166, 2014, p. 116

[670] La proporcionalidad a partir de ahora se calculará también en función del caso dependiendo del caso y proporción al volumen de negocio total anual global del ejercicio financiero anterior. En esta línea, CORRAL (pp. 578) señala lo criticado que fue el régimen de la antigua LOPD, "sobre todo por la cuantía de sus multas, que llegaron a calificarse de inconstitucionales por atentar contra el principio de proporcionalidad" (Vid. Tornos Más, J., "Potestad sancionadora de la AEPD y principio de proporcionalidad", en "Potestad sancionadora de la AEPD", Thomson Aranzadi, 2008, p.33). Y es que como bien señala, "ya no se puede medir la proporcionalidad de las multas utilizando los criterios establecidos por nuestra jurisprudencia constitucional (Stc 65/196, de 22 de Mayo; 160/1987, de 27 de octubre entre otras) sino los que en su caso fije el Tribunal de Justicia de la Unión (que reconoce el principio de proporcionalidad de las multas administrativas; asunto C-255/14).

de las disposiciones normativas. Aunque el art. 83 en sus apartados 4 y 5, no hace mención específica a cuantías mínimas, prevé la posibilidad de sancionar las infracciones cometidas con respecto al tratamiento de datos de carácter personal con multas administrativas de 10.000.000 o 20.000.000 de euros, o en el caso de que se trate de una empresa, de una cuantía equivalente al 2% o al 4% como máximo del volumen de negocio anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

Si profundizamos respecto a la tipificación del la norma europea, podemos echar en falta un articulo, tal y como señala CORRAL (2016, 579), en el que se incluyeran expresamente cada una de las conductas constitutivas de dichas infracciones sino que lo se produce una remisión a otros preceptos . Por otro lado, también existen problemas (mayores), como señala el autor, en la delimitación que el Reglamento realiza de cada sanción es excesivamente amplia.

Es llamativo por otro lado, que en el RGPD no haya previsión regulatoria alguna referente a algún régimen de prescripción (CORRAL, 2016,280).

d. Sujetos involucrados.

Según CORRAL (2016,576) , con el RGPD, se "amplían los sujetos pasivos de la relación jurídica sancionadora al establecer, el art. 83.4 la posibilidad de imponer sanciones no sólo a los responsables y encargados sino también a los organismos de certificación por la vulneración de los artículos 42 y 43, y a los organismos de certificación por la vulneración de obligaciones a las que se refiere el artículo 41.4 del Reglamento".

En segundo lugar, me gustaría señalar dos cuestiones importantes antes de concluir esta cuestión;

i. *Respecto a las AAPP.* Las cuales también están sometidas a las obligaciones recogidas en la norma, aunque no están sometidas al régimen sancionador de las personas privadas y por ello, no se les impone multa administrativa. No es una novedad como sabemos ya que estaba contemplado en la antigua LOPD (art. 46) y reglamento de desarrollo (art.129). Ahora bien, con la llegada del RGPD (Art. 83.7) parece "mantenerse puesto que deja a los EEMM libertad para establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a las autoridades y organismos públicos". Hay quien considera que la RGPD puede resultar "discriminatoria" ya que las AAPP no son sancionados. Es el caso "Belgio",

la asociación que agrupa a la FEB industria belga/VBO , la cual ha apelado contra la ley de aplicación del RGPD ante el Tribunal Constitucional Belga[671].

ii. *Respecto el apercibimiento y advertencias* (Art. 58 RGPD). Este precepto posibilita a las autoridadades de controlar para sancionar mediante *"advertencia"* a los responsable o encargados cuando las operaciones "puedan" infringir el RGPD. Y por otro lado, también se prevé que las autoridades de control sancionen mediante "*apercibimiento*"[672] las operaciones que "hayan infringido" lo dispuesto en el RGPD. Hay que tener en cuenta que estas medidas podrían ser interpuestas a la misma vez[673].

7.2.El régimen sancionador en la LOPDGDD.

Hay que tener en cuenta y avisar al lector del carácter de "Directiva europea" que adopta en ocasiones el RGPD, en tanto que deja bastante margen de maniobra a los EEMM para desarrollar la norma; este es el caso del régimen sancionador. A priori, podemos reconocer que el régimen sancionador español es uno de los más duros antes de la llegada de la norma europea por lo que en principio no ha sido complicada la adaptación en ese sentido. No obstante, se han producido cambios de interés. En la antigua LOPD (art. 44) se regulaban tres grados de infracción**:** leve, grave y muy grave y cada una de ellas prevé un rango de sanciones diferente que variará teniendo en cuenta la graduación anteriormente mencionada.

Respecto a la *sanciones y tipificaciones*, la LOPDGDD aprovecha el artículo 83.2 del RGPD (ref. factores agravantes o atenuantes) para aclarar que entre los elementos a tener en cuenta podrán incluirse los que ya aparecían en el artículo 45.4 y 5 de la antigua LOPD. Por su parte, el art. 77 LOPDGDD[674], perfila el régimen sancionador de las AAPP.

---

[671] Vanin, N. [Nicola Vanin]. (20 de marzo, 2019). #Belgio, l'associazione che riunisce le industria belghe hashtag#FEB/ VBO ha presentato ricorso contro la legge che attua il Regolamento generale sulla protezione dei dati dell'UE hashtag#GDPR presso la corte costituzionale. [Tuit]. Recuperado de https://www.linkedin.com/feed/update/urn:li:activity:6514046252794155008/

[672] No supone una novedad puesto que ya estaba incluido en la antigua LOPD.

[673] CORRAL (2016, 583), no obstante, señala que no existiría problema alguno siempre que las multas administrativas se impongan con carácter sustitutivo y no, con carácter adicional, puesto que se produciría un caso de imposición de doble sanción (o un supuesto de aplicación de *principio non bis in idem*)

[674] "1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados: a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos. b) Los órganos jurisdiccionales. c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local. d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas. e) Las autoridades administrativas

La intención del legislador nacional es adoptar un sistema similar al que regulaba la antigua LOPD, no sancionando con multas pecuniarias a las Administraciones públicas que infrinjan la normativa de protección de datos, sino utilizar la *vía del apercibimiento*[675].

En otro orden de cosas, es de interés mencionar que esta Ley (Titulo X) acomete la tarea de reconocer y garantizar un elenco de *derechos digitales* de los ciudadanos conforme al mandato establecido en la Constitución, y que estarán bajo el régimen sancionador aplicable. A continuación y a modo de conclusión, señalamos el siguiente cuadro diferenciador de las normas y sus disposiciones en materia de sanciones:

Norma Aplicable	**Sanciones**		
	Leve	**Grave**	**Muy grave**
LOPD/RLOPD *(Antes)*	900 € - 40.000 €	40.001€-300.000€	300.001-600.000€
RGPD *(Ahora)*	No se establece un rango mínimo de cuantía	Multa administrativa de hasta 10.000.000€ o, en el caso de empresas, de cuantía equivalente al 2% como máximo del volumen de negocios total anual global del ejercicio financiero anterior, lo que resulte mayor en cuantía.	Multa administrativa de hasta 20.000.000€ o, en el caso de empresas, de cuantía equivalente al 4% como máximo del volumen del negocio anual global del ejercicio financiero anterior, lo que resulte en mayor cuantía.

Tabla 39. Cuadro comparativo sanciones LOPD/RGPD

8. EL DERECHO A INDEMNIZACIÓN Y RESPONSABILIDAD.

independientes. f) El Banco de España. g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público. h) Las fundaciones del sector público. i) Las Universidades Públicas".

[675] Diario de Navarra. (22 de febrero de 2012). Salud debe pagar 125.000 euros por acceso ilegítimo historial una paciente. https://www.diariodenavarra.es/noticias/navarra/mas_navarra/salud_debe_pagar_125_000_euros_por_acceso_ilegitimo_historial_una_paciente_70815_2061.html

La existencia de la institución de la indemnización, que tiene su origen en el derecho romano, es imprescindible en cualquier Estado de Derecho, ya que empodera al perjudicado y le otorga el derecho a la tutela judicial efectiva.

En materia de protección de datos, no se trata de una previsión novedosa para nosotros puesto que la antigua LOPD (art. 19) ya lo preveía para personas físicas a través de una acción por responsabilidad civil siempre que se sufriera un daño o lesión en sus bienes o derechos. Con la antigua Directiva europea (art. 23) se introdujo un mandato a los legisladores nacionales para que reconocieran dicho derecho, pero dado que se trataba de una transposición en los ordenamientos internos cada legislación nacional lo transponía según le interesaba. Ahora, con el artículo 82 del RGPD, por primera vez se regula este derecho en el marco de una norma europea homogeneizando el escenario regulatorio en los EEMM. La creación de un sistema de indemnización por la infracción de un derecho fundamental a nivel de la UE "pone de manifiesto, de nuevo la consolidación de la Carta de Derechos Fundamentales de la Unión como motor de integración jurídica europea" (NIETO, 2016, 569).

Es decir, al margen de aplicar el régimen sancionador, podrán ser declarados a los responsables y encargados de tratamiento como "responsables de la lesión" y en su caso, deberán indemnizar al perjudicado (art. 83 y 84 así lo prevé aunque haya remisión a la legislación nacional). Según Nieto (2016, 555)[676], podríamos señalar lo siguiente:

Sanciones Administrativas	**Indemnización**
- Se representa en *Ius ponendi* del Estado. - Finalidad *preventiva.*	La institución de la acción resarcitoria del daño, de la responsabilidad civil o en su caso, patrimonial de la Administración tiene una finalidad de *resarcimiento* al perjudicado de los daños y perjuicios sufridos por el tratamiento ilegal de sus datos.

Tabla 40. Diferencias entre sanciones administrativas e indemnización.

A continuación, nos detendremos únicamente en analizar el derecho de indemnización y del sistema de responsabilidad del art. 82, titulado "derecho a

[676] NIETO GARRIDO, Eva, "Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad" Dtor. J.L. Piñar, 2016, en "Derecho a indemnización y responsabilidad". Página 555.

indemnización y responsabilidad[677]" y sus ocho características según NIETO (2016, 557-565):

a. *Protección uniforme y de obligado cumplimiento para los EEMM*. Sobre ello hemos hablado anteriormente.
b. *Régimen general* (toda actividad fáctica o jurídica o inactividad del responsable del tratamiento). Es decir se refiere a toda operación que no cumpla por acción u omisión el RGPD, también los actos delegados y de ejecución adoptados de conformidad con el RGPD, así como las normas de desarrollo (considerando 146).
c. *Sistema de responsabilidad directa* tanto si lo realizó el responsable como si lo realzara el encargado. Aunque la responsabilidad de este último sea más limitada puesto que responde solo por los daños causados por incumplimiento del RGPD, o de normas derivadas o bien por que desobedezca al responsable.
d. *Responsabilidad subjetiva* que exige la concurrencia del dolo, culpa o negligencia lo que incluye la culpa *in vigilando*[678]. El art. 82.3 exonera de responsabilidad por los daños causados en la operación del tratamiento al responsable y/o encargado cuando demuestren "que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios".
e. *Reparación integral*. Así lo señala el art. 82.2 que garantiza una reparación que cubra no sólo los daños físicos y patrimoniales sino también los *daños morales* (al igual que la LGCYU). Además, la autora señala acertadamente, "aunque el art. 82 no lo mencione el daño habrá de ser efectivo y real, evaluable económicamente e individualizable con relación a una persona o grupo de personas, al igual que sucede en el derecho interno" (art. 32.2 Ley 40/2015). La autora referencia

[677] Existen diferencias entre los términos anglosajones "responsability", "liability" y "accountability":
- Según el Diccionario de *Oxford English* define la responsabilidad ("*responsability*") como "un cargo, fideicomiso o deber, por el cual uno es *responsable*. Se define como responsable ("*answeable, accountable*") a aquellos que son susceptibles de ser llamados a *rendir cuentas* o también *capaces de cumplir una obligación o un fideicomiso*.
- Según el Diccionario de la Academia de *Cambridge*, la responsabilidad ("*liability*") es "la responsabilidad de una persona, empresa u organización de pagar o renunciar a algo de valor". Se entiende por ("liability") a "la condición de ser responsable o estar sujeto a la ley" (Onions,1984) Vid. CORNOCK, Marc (2014) https://oro.open.ac.uk/49089/3/Legal%20principles%20of%20responsibility%20and%20accountability%20in%20healthcare.pdf
- Por su parte, responsabilidad ("accountability") supone la responsabilidad que no se limita únicamente a designar quién es el responsable de una acción, sino que también exige que la persona que realiza la tarea pueda rendir cuentas o explicaciones o motivos de esa acción (Cornock, 2011,25). Conock señala que "la *accountability* denota profesionalidad y es un estándar más alto que la *responsability"*, también afirmó que "solo la *accountability* se puede delegar a los demás, la *responsability* no se puede delegar". Vid. CORNOCK, Marc (2011) Definiciones legales de responsabilidad, responsabilidad y responsabilidad.

[678] La autora señala algo muy importante: en nuestro sistema español el principio de responsabilidad subjetiva se aplica a derecho civil y penal pero no, a derecho administrativo a diferencia del resto de países de nuestro alrededor. No obstante, con el RGPD "el derecho de indemnización resulta acorde con la responsabilidad subjetiva, por dolo, culpa o negligencia y que es la aplicable para exigir la responsabilidad extracontractual de las instituciones y organismos de la UE.

a ABERASTURI[679], señalando que "en ocasiones, cuando el daño ha sido hipotético o no se ha producido, por el poco tiempo en que los datos estuvieron expuestos, los tribunales han denegado la indemnización considerando que la reparación de la lesión del derecho fundamental se ha producida con la Sentencia declarativa". Mientras que con la LO 1/1982 de protección civil del derecho al honor, la intimidad personal y familiar y la propia imagen se presumía[680] (art. 9.3) la existencia del perjuicio siempre que se acreditara la intromisión ilegítima, ahora con el RGPD (art. 83) se deberá "probar la existencia del daño aducido, y además, la relación de causalidad entre la acción u omisión del responsable con el daño producido.

f. *Responsabilidad solidaria* del responsable y encargado (art. 82.4 y 5). El perjudicado tiene la posibilidad de acudir bien a uno o al otro para exigirle "el abono del total de la indemnización". Quien abonó el total de la indemnización podrá repetir contra al resto de los sujetos responsables por la parte que corresponda. Este precepto tiene el objetivo de garantizar la indemnización efectiva del interesado.

g. *Acción de reclamación de responsabilidad por daños.* [681][682]

A continuación me gustaría señalar una cuestión de sumo interés; y tiene que ver con la *evolución e inclusión del procedimiento de responsabilidad por daños y perjuicios en el régimen sancionador en el ámbito de derecho administrativo.*

---

[679] ABERASTURI GORRAÑI, Unai, "El derecho a la indemnización en el art. 19 LOPD", Revista Aragonesa de la Administración Pública núm. 41-2, 2013, pp.180 a 186. "En otros supuestos, cuando la lesión del derecho fundamental a la protección de datos de carácter personal va unida también a la lesión del derecho fundamental al honor, intimidad e imagen, los órganos judiciales acuerdan una indemnización conjunta (STS de 16 de marzo de 2016, Sala Primera, ponente Magistrado Rafael Saraza Jimena, recurso de casación núm. 3269/2014)

[680] También en la Ley General para la Defensa de Consumidores y Usuarios que en su art. 48 permite la indemnización de daños y perjuicios probados causados al consumidor. A pesar de ello, igual que ocurre en el RGPD, no se ha llevado a la práctica esta posibilidad.

[681] El legislador europeo ha optado "por dar la opción al perjudicado de los EM donde el responsable o encargados tenga su establecimiento, sino además permitir que la acción de reclamación se presente ante l os tribunales competentes del Estado miembro donde el perjudicado tenga su domicilio". Según la autora, se trata, sin duda de un gran avance en la tutela del derecho fundamental (…) que elimina el obstáculo que suponía para la efectividad del derecho a una indemnización el tener que acudir a reclamar la misma a otro EM, distinto de aquel donde el perjudicado tuviese su domicilio, porque el responsable o el encargado tenía allí su establecimiento.

[682] Es necesario en este punto distinguir entre el proceso administrativo y el procedimiento civil. En el ámbito de derecho administrativo, nos referimos cuando el responsable de la actividad de tratamiento de datos personales sean las AAPP (vid. Art. 2 y 67 Ley 39/2015), en el cual los interesados solo podrán solicitar el inicio de un procedimiento de responsabilidad patrimonial *antes de transcurrir el año* de producido el hecho o el acto que motive la indemnización o se manifieste su efecto lesivo. Y en el ámbito del procedimiento, en el art. 1968 regulará el plazo previsto para la acción para exigir la responsabilidad civil por las obligaciones derivadas de la culpa o negligencia, los cuales prescribirán *al año* desde que lo supo el agraviado. Y si tenemos en cuenta la LO 1/1982, de 5 de mayo, que regula el plazo de interposición de la acción frente a intromisiones ilegítimas al derecho a la intimidad y a la protección de datos personales, en concreto, el art. 9.5, el plazo se erige en *4 años* desde que el legitimado pudo ejercitarlas.

Los antecedentes de este derecho de indemnización se pueden encontrar en otras normas existentes. La LO 1/1982 con su art. 9.3 fue la primera norma en nuestro Derecho en reconocer, a nivel legislativo, la indemnización de los daños morales, con independencia de que el hecho dañoso fuera o no constitutivo de delito. También la Ley General de Consumidores y Usuarios (LGCYU) en su art. 128 contemplaba este derecho a la indemnización y hace 5 años, por su parte, la Ley 40/2015 en su art. 28.2 recogía la posibilidad de que el órgano sancionador estableciera la indemnización por daños y perjuicios. Por tanto, podríamos decir que nos encontramos en un nuevo paradigma de la institución indemnizatoria. Esta afirmación es compartida por el autor *Huergo Lora*[683].

Este autor señala que esta institución no se contemplaba de estar contenida en la resolución administrativa por la que se impone una sanción y además se incluye la condena al infractor a abonar una indemnización a países como Alemania o Italia, y que en todo caso, España ha ido tomando como referencia al sistema penal donde se contemplaba, aquí sí, la posibilidad de incorporar la indemnización para resarcir a perjudicados. Ahora bien, *¿la responsabilidad civil derivada de la infracción supone desplazar al juez?* La respuesta es negativa para el autor, puesto que considera **que** lo que se produce es un cambio de "la intervención del juez civil por la del contencioso-administrativo**".** Para él no sólo se trataría de un "cambio orgánico" donde el juez contencioso declara la responsabilidad civil, sino que afirma que lo que "existe es una exigencia de habilitación legal expresa para que la Administración pueda no sólo sancionar, sino decidir la responsabilidad civil".

[683] Para más info ver en: https://almacendederecho.org/sanciones-administrativas-y-responsabilidad-civil/ "Parece claro que con esta nueva regulación se pretende que la resolución sancionadora pueda pronunciarse sobre la responsabilidad civil del infractor (es decir, sobre la indemnización que debe pagar al perjudicado por la infracción) y que ese pronunciamiento tenga la misma fuerza que el resto del contenido de la resolución, lo que significa que será vinculante, podrá ser objeto de ejecución forzosa por parte de la Administración y quien no esté de acuerdo con él tendrá que impugnarlo en vía contencioso-administrativa".

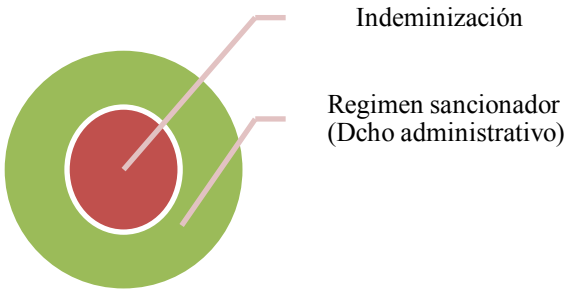


Imagen 66. Esquema Reg. Sancionador vs institución de la indemnización.

Otra cuestión nada baladí tiene que ver con la dificultad de cuantificar el daño y la indemnización[684] para las AAPP, o más concretamente, para las autoridades de control nacionales como la AEPD. Podemos entrar en un terreno pantanoso al acercar las competencias administrativas al poder judicial, pero acaso, ¿no podrían las autoridades de control resolver cuestiones indicando y sancionando con indemnizaciones para resarcir el daño a los perjudicados en vulneraciones del derecho fundamental de protección de datos? *Huergo*, en este sentido, señala que "es la imposición de una sanción la que permite que alguien (la Administración o los tribunales civiles, da igual) imponga también la responsabilidad civil, sin que puedan existir resoluciones "contradictorias". Si bien es cierto, la pericia del Juez es esencial, quizás, se podría realizar unos baremos prefijados por las autoridades (sobre todo pensando en indemnizaciones con cuantías bajas), evitando además con ello, el coste económico que supone al perjudicado acudir a sede judicial civil. En mi humilde opinión, la tendencia parece ir en la línea de este acercamiento competencial de la sede administrativa con la judicial, motivado principalmente por la sobrecarga de trabajo que posiblemente vayan recibiendo las autoridades de control a partir de ahora con la nueva norma en vigor.

Por último, no quisiera perder la oportunidad de hablar brevemente como quedaría el escenario tras la entrada en vigor de la nueva LOPDGDD en diciembre de 2018. Aunque se esperaba una adaptación con articulado expreso donde se pudiera actualizar el art. 19 de la antigua LOPD (y concretamente se extendiera el ámbito de aplicación

[684] Para NIETO (2016, 568) aplicando analógicamente las normas que rigen las responsabilidad patrimonial de las AAPP, "el daño habrá de ser efectivo, real y cierto; evaluable económicamente, lo que será más difícil pero no imposible en el caso de daños morales..."

más amplio), el RGPD como norma europea de aplicación directa a los EEMM con el art. 82 ha venido a regular esta institución indemnizatoria de igual modo, permitiendo que "cualquier perjudicado acuda a los tribunales nacionales, bien civiles, bien contencioso-administrativos, ejercitando su acción de reclamación por daños por infracción del propio RGPD o los actos derivados del mismo" (NIETO, 2016,655)[685].

Esta autora considera que "es excesivamente genérica e insuficiente en concretar algunos aspectos de los requisitos que deben cumplirse para reclamar la indemnización[686]" y además, considera que " hasta ahora la aplicación de las normas que regulan la responsabilidad civil por daños (art.1106 CC), así como la responsabilidad por daños en otros derechos fundamentales como el derecho al honor, a la intimidad personal y familiar y a la propia imagen (Art. 9, LO 1/1982) y la responsabilidad patrimonial de las AAPP (art.32-7, Ley 40/2015), han permitido delimitar las características del sistema interno de responsabilidad por daños y el derecho a indemnización por el tratamiento ilícito de los datos de carácter personal[687].

[685] NIETO, considera que hubiera sido positivo (tengamos en cuenta que su artículo data del 2016, previamente a la entrada en vigor de la nueva LOPDGDD) que "el legislador orgánico (*de lege ferenda*) que reforme LOPD para adaptarla al RGPD incluya, además de lo dispuesto en el citado RGPD, las características del derecho a la indemnización y la acción de reclamación que constituyen doctrina y jurisprudencia consolidada.

[686] ABERASTURI GORRIÑO, Unai "El derecho a la indemnización el art.19 de la LOPD" P.176. Recuperado de http://w.aragon.es/estaticos/GobiernoAragon/Organismos/InstitutoAragonesAdministracionPublica/Areas/03_Revista_Aragonesa_Formacion/04%20Unai%20Aberasturi.pdf

[687] PUYOL MONTERO, Javier "Derecho a indemnización", Troncoso Reigada,Antoni (dir), "Comentarios a la LOPD, Cviitas y Thomson-Reuters, Cizur Menor, pp. 1263 y ss.

CAPÍTULO VI. EL DERECHO FUNDAMENTAL DE LA PROTECCIÓN DE DATOS PERSONALES. ENFOQUE DESDE EL ÁMBITO DE LA SALUD Y TECNOLOGÍA

SUMARIO: 1. 1.INTRODUCCIÓN.- 2. EL DERECHO DE PROTECCIÓN DE DATOS COMO DERECHO DE LA PERSONALIDAD.- 3. BREVE ORIGEN DOCTRINAL Y JURISPRUDENCIAL DE LA PROTECCIÓN DE DATOS PERSONALES. - 4. LA IMPORTANCIA DEL DERECHO DE PROTECCIÓN DE DATOS DE SALUD DIGITAL EN LA ERA TECNOLÓGICA.

"Si los derechos fundamentales se eliminan por el dinero y la democracia cede a la dictadura, dentro de poco nadie será libre"

(Stefano Rodotà)

1. INTRODUCCIÓN.

A continuación diferencieramos los siguientes conceptos entre sí desarrollando y analizando su origen y particularidades especiales:

El derecho a la intimidad	**El derecho a la privacidad**	**La autodeterminación informativa o "habeas data"**	**El derecho a la protección de datos personal**
-Se extiende sobre un espacio muy reducido: al ámbito de la persona. -Otorga al sujeto titular el poder jurídico negativo de limitar a terceros, públicos o privados, cualquier injerencia o intromisión	-Se extiende sobre un espacio más amplio que el de la intimidad en el que se incluyen los datos personales de dicha persona. -Es el derecho a decidir cuándo, cómo y en qué medida la información	-Es la *facultad general* de disponer de los datos propios imponiéndolos a terceros. -El titular tiene derecho a conocer los datos referidos a sí mismo y la finalidad para la que están	-Reconoce al ciudadano la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos. -Este derecho se centra en el deber de *acciones positivas* que recae

en su esfera íntima.	personal es comunicada a los otros, esto es lo que él denomina *autodeterminación informativa*[688]. En definitiva, es la capacidad individual de control del flujo de información personal. -Es una necesidad que urge a los particulares como consecuencia de las presiones que ejerce la vida en sociedad en el actual *entorno tecnológico* sobre su ámbito íntimo (Solove)	siendo tratados por un determinado responsable, pudiendo en su caso instar su *rectificación, cancelación o actualización.*	tanto sobre los *poderes públicos como sobre los agentes privado.*[689]

Tabla 41. Diferencias conceptuales entre derecho a la intimidad, privacidad, habeas data y protección de datos.

Respecto al *derecho a la intimidad,* hemos de decir que la tradición filosófica inglesa (que arranca con *Thomas Hobbes* y *John Locke*) contribuyó a definir el concepto anglosajón de "*privacy"* y a buscar un equilibrio entre las acciones del Estado y el individuo. En todo caso, como sostiene Pérez Luño[690], "en nuestra época resulta insuficiente concebir la intimidad como un derecho garantista (*status negativo*) de defensa frente a cualquier invasión indebida de la esfera privada, sin contemplarla, al propio tiempo, como un derecho activo de control (*status positivo*) sobre el flujo de

[688] WESTIN, A. F., (1967) Privacy and Freedom, New York, Atheneum, pág. 7. Vid. Saldaña, M. N., "La protección de la privacidad en la sociedad tecnológica..." op. cit. pág. 99

[689] Thompson, J. B., "Los límites cambiantes de la vida pública y privada", op. cit. pág. 33. (El autor señaló ; "Lo privado hoy está constituido por un territorio "desespaciado" de información y contenido simbólico sobre el cual cada individuo piensa que puede ejercer control sin que sea relevante dónde este individuo o esta información se sitúen fisicamente". Y es que cuando una persona se encuentra en su casa y se conecta a Internet para revelar información sobre el mismo además de encontrarse en el "espacio *privado* de su hogar", a la misma vez, está participando en un *entorno público de difusión de la información* donde la actividad informática permite la concentración de datos en un espacio ilimitado. El constituyente previó ya en 1978 una garantía jurídica especial al tratamiento de la información personal en el ámbito concreto de *la informática* (Art. 18.4 CE)).

[690] PEREZ LUÑO, A. E., Derechos Humanos, Estado de Derecho y Constitución, op. cit. pág. 330.

informaciones que afectan a cada sujeto". Este concepto de derecho a la intimidad debe evolucionar con el fin de superar de las deficiencias que adolece para afrontar las nuevas amenazas[691].

En segundo lugar, hemos señalada al *derecho a la privacidad* consiste en el derecho de los individuos a una esfera privada de no injerencia y al control sobre los aspectos relacionados con su vida. Solove[692] estableció que la privacidad es un derecho determinado y no abstracto y una necesidad que urge a los particulares como consecuencia de las presiones que ejerce la vida en sociedad sobre su ámbito íntimo, de manera más apremiante en el actual entorno tecnológico relacionado con los nuevos sistemas de información y comunicación. En definitiva, la noción de privacidad, es difícil de precisar dada la influencia de distintos factores contextuales: sociales, circunstanciales y en nuestros días, tecnológicos.

En tercer lugar, hablemos de autodeterminación informativa. Por su parte, Westin contribuyó a la delimitación de la *privacidad* como "*control*"[693] de la información de uno mismo, definiendo la privacidad como el derecho a decidir cuándo, cómo y en qué medida la información personal es comunicada a los otros, denominándolo "*autodeterminación informativa*"[694]. Rössler distingue tres esferas de la privacidad: (i) privacidad *informativa*, que consiste en el control de la información sobre sí mismo y el derecho a protegerla del acceso indeseado de los demás; (ii) privacidad *de decisión*, que implica el control de nuestras decisiones y acciones; (iii)

[691] Ver SOLOVE, D. J., "A Taxonomy of Privacy", op. cit. pp. 523-548. Para el experto en privacidad Solove, hay cuatro ámbitos donde aparecen nuevos desafíos para preservar la intimidad, sin animo de que sea una clasificación exhaustiva: 1) Recopilación de información; 2) Procesamiento de información; 3) Diseminación de información; 4) Invasión. El propósito de esta taxonomía es examinar los peligros que entrañan estas actividades en cada contexto para categorizarlas y posteriormente buscar posibles soluciones. Ver SOLOVE, D. J., "A Taxonomy of Privacy", op. cit. pp. 523-548

[692] Ver SOLOVE, D. J., 2008, Understanding Privacy, Cambridge, MA: Harvard University Press.

[693] Según un estudio de Accenture, el 30% de e-pacientes encuestados tiene acceso a su HCE, pero el 89% de los pacientes crónicos sienten que no tienen control de los mismos. La cuestión más llamativa es que los consumidores y e-pacientes crónicos no sienten tanta preocupación por la invasión de la privacidad en su HCE o datos electrónicos de salud que en situaciones como las del comercio electrónico. Ver en https://www.accenture.com/t20150708T033735__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Industries_11/Accenture-Consumers-with-Chronic-Conditions-Electronic-Medical-Records.pdf#zoom=50

[694] Westin, A. F., 1967, Privacy and Freedom, New York, Atheneum, pág. 7. Vid. Saldaña, M. N., "La protección de la privacidad en la sociedad tecnológica..." op. cit. pág. 99

privacidad *espacial*, el control respecto a nuestros propios espacios y el derecho a protegerlos de la intrusión indeseada de los demás[695] [696].

En cuarto lugar, sería conveniente diferenciar claramente el derecho que acabamos de explicar respecto del "derecho de protección de datos personales". Ambos se deben entenderse como complementarios; el derecho a la autodeterminación informativa tiene la función de *garantizar* a los ciudadanos unas facultades de información, acceso y control de los datos que les conciernen mientras, el derecho a la protección de los datos de carácter personal se centra en *el deber de acciones positivas* que recae tanto sobre los poderes públicos como sobre los agentes privados, de otorgar efectiva protección a los datos personales que obran en su poder, desde el momento en que éstos son recabados hasta que son cancelados por haber cumplido ya su finalidad. De ahí que el derecho de protección de datos se deba entenderse como la *"tutela jurídica de los datos personales"* operada a través del derecho a la autodeterminación informativa y del derecho a la intimidad. El Tribunal Constitucional, prefiere referirse a este derecho como la "libertad informática", consagrando con ella un derecho de control sobre los datos relativos a la propia persona (vid. SSTC 254/1993, de 20 de julio o 292/2000, de 30 de noviembre).

A continuación, analizados los cuatro derechos anteriores, procederemos a detenernos a en el derecho fundamental de protección de datos como derecho de la personalidad.

2. EL DERECHO DE PROTECCIÓN DE DATOS COMO DERECHO DE LA PERSONALIDAD

Como venimos diciendo, el derecho a la protección de datos y la privacidad es un derecho humano (art. 12. Declaración Universal de los Derechos Humanos de 1948) y un derecho fundamental en virtud de nuestra constitución española (Art. 18.4 CE).

[695] Rössler, B., 2005, The value of privacy, Cambridge: Cambridge Polity Press. Ver Thompson, J. B., "Los límites cambiantes de la vida pública y privada", op. cit. pág. 30.

[696] Las violaciones a la privacidad en cada una de estas dimensiones se traducen en hechos ilícitos como son el acceso y uso ilícito de información o en intrusiones ilícitas en los espacios privados (como internet) bien sea por medio de vigilancia o a través de las nuevas tecnologías. Estos hechos estarán tipificados en nuestro Código Penal en el art. 197 y ss.

Pero también se le puede considerar como un derecho de la personalidad en tanto que garantiza a la persona el goce de sus bienes, protegiendo sus atributos físicos, morales y su libre desarrollo y ejerce el control sobre los datos personales. Por tanto, nuestro derecho tiene encaje dentro del grupo de derechos de la personalidad que protege el ámbito moral de la persona. Para BATUECAS (2015), el derecho a la protección de datos deberá ser entendido en su calificación jurídica como un *desarrollo del derecho a la intimidad personal.*

Es claro que el derecho fundamental de protección de datos no se puede entregar, transferir o vender. Los derechos humanos son derechos intrínsecos y evidentes por sí mismos, al margen de que estén envueltos y protegidos por regulación.

No obstante, el hecho de que *derechos personalísimos* como el derecho de intimidad o protección de datos sea intransferibles no implica que el titular de los mismos no pueda realizar "negocios patrimoniales" de algún tipo. Los derechos de la personalidad están vinculados a la persona y afectan a bienes de carácter no estrictamente material, pero pueden ser susceptibles de una "valoración cuantitativa económica" como si se tratara de una "reparación" o "compensación económica" ("royalties") por el uso o utilización de los mismos por organizaciones o entidades (públicas, para el bien común[697] o privadas, para el interés empresarial). BATUECAS (2015) ya decía; "… en el ámbito próximo de la intimidad se admite la realización de negocios patrimoniales sin que ello varíe su calificación" . A mi modo de ver no sería necesario que se incluyera dentro del bloque de derechos patrimoniales el resultado de estas "compensaciones".

La abogada RENIERIS (2018) señalaba que: "Los datos transmiten liquidez y transferibilidad y una vez digitalizados, los datos sobre nosotros (es decir, los datos personales) se convierten en *dinero* y adquieren una calidad transferible o transaccional"[698].

Por tanto, se podría dejar abierta la posibilidad de que "algunos" datos personales podrían existir en alguna forma similar de quasipropiedad. Imaginemos por un momento que pudiéramos *cambiar "datos" por "medicamentos"* o *"datos" por "servicios de*

[697] *Christopher Olk*, los datos más que ser un producto de cada individuo pertenecerían a la sociedad entera.
[698] Vid. https://medium.com/@hackylawyER/money-talks-how-digital-money-speech-challenge-existing-legal-frameworks-dd845a7ceaf7

salud privados" (tele consulta, etc.). Ceder información personal a cambio de una retribución, descuentos o similar cada vez es más posible, y más aún, con la expansión de la tecnología *blockchain* y DLT en la Industria de la Salud[699], o pensamos en la posibilidad de empoderar al individuo otorgándole herramientas para gestionar los datos y monetizar datos personales[700]. No obstante, tengamos en cuenta que si se trata de "venta" o "alquiler" de datos personales de salud agregados o anonimizados, no se considerarían datos personales por la norma europea. Dicho todo ello, hay que tener ciertas precauciones y consideraciones:

i. La concepción del dato como propiedad -que puede ser vendido, comprado o alquilado- podría derivar a lo que denomina esta autora como *"modelo de tecnología publicitaria de Internet"* (RENIERIS)[701]. Esta situación puede resultar algo peligrosa si la tendencia acaba convirtiéndose convertirse en un modelo extendido a todas las facetas de nuestra identidad digital.

ii. El significado de los datos es algo de lo que la persona que los genera datos no podría/debería separarse por completo. No obstante, sino somos dueños de los datos debemos tener, al menos, la capacidad de comprender la importancia de transferir esos datos en la medida en que los datos puedan utilizarse para beneficiarnos, perjudicarnos, exponernos o protegernos.

iii. "Internet y la *identidad digital* obligan a redefinir los derechos fundamentales de la persona y el concepto mismo de personalidad, admitiendo vertientes de ésta inexistentes hasta hace poco tiempo" (BATUECAS, 2015). En definitiva, Internet ejercerá una influencia directa en el desarrollo de la personalidad de las personas ahora y en el futuro. El autor añade; "de igual manera que la *libertad personal* resulta esencial para

[699] La empresa española *PrivacyCloud* ha desarrollado *Werule,* una aplicación móvil que permite cambiar información personal por servicios[699]. *Spotify*, por ejemplo, usa esa plataforma y permite que el usuario decida compartir información como la edad, el estado civil o sus gustos concretos, y a cambio proporciona al usuario puntos canjeables para los usuarios.

[700] Como más adelante trataremos, eso es posible con aplicaciones como CitizenMe, People.op, Hat Community Foundation, CTRL.io, Cozy.io, Digi.me o Meeco.

[701] Vid. https://medium.com/@hackylawyER/do-we-really-want-to-sell-ourselves-the-risks-of-a-property-law-paradigm-for-data-ownership-b217e42edffa

que el hombre vea satisfecho el libre desarrollo de su personalidad en su vida diaria, así también viene a serlo la protección de datos en el entorno digital".

Hay que tener en cuenta, además, que los derechos aunque son evidentes *nunca se han ejecutado por sí mismos*. A continuación, analizado todo lo anterior, procederemos a estudiar el origen doctrina y jurisprudencial del derecho de la protección de datos como derecho fundamental en el ámbito europeo, español y americano.

3. BREVE ORIGEN DOCTRINAL Y JURISPRUDENCIAL DE LA PROTECCIÓN DE DATOS PERSONALES.

3.1.Recorrido histórico doctrinal y jurisprudencial sobre la privacidad europea.

El artículo 8 del CEDH pretende garantizar una esfera de la vida del individuo en la que el mismo pueda desarrollar libremente su personalidad y disponer libremente de sus actos, sin interferencias de los poderes públicos. Las primeras sentencias en las que el TEDH se pronunció sobre la cuestión son sentencias en casos relativos a ***escuchas telefónicas***[702]. Por otro lado, el concepto de "datos personales" y se amplía, refiriéndose no sólo a la vida privada, sino también a cualquier otro dato relativo a la *vida pública* de una persona siempre que afecte al *desarrollo de su personalidad* (Sentencia de 4 de mayo de 2000, caso Rotaru[703]). El Tribunal comenzó a referirse a determinados datos personales como *datos sensibles*, por ejemplo, aquellos que afectan más directamente al *desarrollo de la personalidad,* como, por ejemplo, el dato relativo a la homosexualidad (Sentencia de 17 Octubre 1986. Asunto Rees c./ Reino Unido; Sentencia de 25 marzo 1992 Asunto B c./ Francia). También se consideran *sensibles* los datos relativos a la ideología política de un individuo o, cuestión que centra nuestro trabajo, los *datos médicos*. Así lo ha dicho el TEDH en la Sentencia del TEDH de 27 de agosto de 1997,

[702] El Tribunal entiende que en estos casos se produce un tratamiento de datos puesto que las escuchas tienen como consecuencia el registro y archivo de las informaciones obtenidas. Así, por ejemplo, podemos citar las SSTEDH de 6 de septiembre de 1978, caso Klass; la de 2 de agosto de 1984, caso Malone; o la STEDH de 8 de abril de 2003, caso M.M. vs. Holanda, , donde se habla de "grabación o interceptación del tráfico de datos a través de infraestructuras de telecomunicación".

[703] TEDH. Sentencia 28341/95, DE 4 DE MAYO DE 2000. Caso Rotaru contra Alemania. Derecho al respeto de la vida privada. Recuperado de http://hudoc.echr.coe.int/eng?i=001-162581

caso M.S. vs. Suecia[704], donde los *datos médicos,* y en concreto, los datos relativos a un aborto, se consideraron por el Tribunal como "datos personales de naturaleza altamente personal y sensibles". Por su parte, en los años ochenta los *avances tecnológicos* comenzaron a permitir que la recogida, almacenamiento y utilización de datos personales se llevara a cabo de una forma antes inimaginable.

En 1983, la Sentencia del Censo del Tribunal Constitucional Alemán recoge de forma expresa el Derecho Fundamental a la *autodeterminación informativa*, en la antes mencionada dirección marcada por Westin en 1967. Han pasado varias décadas desde que ese Tribunal decidió, en el marco de las protestas populares contra el censo, *que no era correcto almacenar información sobre los ciudadanos de forma ilimitada.* En su sentencia, el Tribunal definió el *derecho a la autodeterminación informativa* como nuevo derecho fundamental autónomo[705]

En Alemania, una sentencia del 2008 de su Tribunal Constitucional, considerada como la fuente del nuevo "*derecho a la integridad y confidencialidad de los sistemas informáticos"*, supone una concreción en la definición de la protección de datos frente a las *nuevas tecnologías.* La sentencia respondió a un recurso presentado contra la reforma de la ley de los servicios de inteligencia del Land de Renania del Norte Westfalia, en virtud de la cual se permitía expresamente que esos servicios pudieran utilizar de forma secreta troyanos para espiar los ordenadores de cualquier sospechoso, lo cual significa entrar en el ordenador, reunir toda la información encontrada y analizarla posteriormente. El Tribunal consideró la reforma como inconstitucional y configuró el nuevo derecho ya mencionado.

Fue, también, el propio TEDH el 24 de junio de 2004 quien declaró en el caso *von Hannover que :*«el incremento en la protección de la vida privada se hace necesario cuando entran en juego las *nuevas tecnologías*, que permiten el almacenamiento y la reproducción de datos personales, como por ejemplo sucede en la toma sistemática de determinadas fotos y su difusión a un amplio sector del público».

---

[704] Se trataba de la comunicación sin consentimiento de la paciente de datos médicos personales y confidenciales de un servicio médico de ginecología a otro tipo prestacional.

[705] Se señaló que; "El derecho a la autodeterminación informativa presupone, también en el marco de las nuevas tecnologías de la información, que cada individuo pueda decidir de forma libre sobre posibles tratamientos de sus datos, así como de poder actuar en función de los mismos. El derecho a las autodeterminación informativa hace imposible la existencia de un sistema social y legal en el que los ciudadanos no puedan saber quién, qué, cuándo y en qué condiciones dispone de información sobre ellos".

3.2.Recorrido histórico doctrinal y jurisprudencial sobre la privacidad española.

Hay dos sentencias españolas significativas en materia de privacidad. La primera de ellas es la ***STC 254/1993***[706], en la que se define por primera vez lo que entonces se denominaría como ***"libertad informática"***[707]. El TC subrayó la importancia que poseía la satisfacción de estos derechos, tomando como referencia el artículo 18 C.E. Y en segundo lugar, se encuentra la ***sentencia 292/2000***[708]**, la cual** consolida la consideración de la protección de datos **como *un derecho fundamental*** como un **derecho netamente** prestacional del que dimanan derechos del afectado **junto con las obligaciones** para el responsable del tratamiento. En otro orden de cosas, y llegados a este punto, es de subrayaren cuenta que el art. 18.4 CE tendrá plena autonomía respecto al derecho de intimidad (art. 18.1 CE).

Derecho a la intimidad	Derecho Protección de datos personales (*habeas data*) / Autodeterminación informativa / Libertad Informática
• **Art. 18.1 CE** • "Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen"	• **Art. 18.4 CE** • "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"

Tabla 42. Diferencias entre preceptos derecho a la intimidad vs derecho a la protección de datos.

Mientras que el derecho de la intimidad se extiende sobre un espacio muy reducido aproximándose al máximo al ámbito de la persona, el derecho de la privacidad delimita un espacio más amplio en el que se incluyen los datos personales de dicha persona. El valor de la intimidad se extiende al círculo de la vida privada o esfera personal, esto quiere decir que en dicha esfera habrán datos de carácter personal

[706] Sentencia del Tribunal Constitucional 254/1993, de 20 de julio de 1993. Recuperado de http://hj.tribunalconstitucional.es/it/Resolucion/Show/2383

[707] El recurso de amparo que dio lugar al pronunciamiento tuvo su origen en la petición de información por parte de un ciudadano vasco al Gobernador Civil de Guipúzcoa sobre la existencia de ficheros automatizados de la Administración del Estado que pudiesen contener datos relativos a su persona. Se solicitaba también, en caso de que éstos existieran, la indicación del organismo estatal en el que se encontraban, la finalidad de los ficheros, la autoridad que los controlase y su residencia habitual y, además, se pedía la comunicación de los datos existentes que le afectasen, de forma inteligible y sin demora. La solicitud fue denegada por la Administración y, agotada la vía administrativa, la denegación fue confirmada por las sucesivas instancias judiciales, interponiéndose finalmente recurso de amparo al Tribunal Constitucional.

[708] Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre de 2000. Recuperado de http://hj.tribunalconstitucional.es/es/Resolucion/Show/4276

"íntimos" y "no íntimos". La *autodeterminación informativa* entra en la escena jurídica para dar cobertura normativa a los datos personales no de carácter íntimo sino de carácter privados. Ese se convierte en su cometido, es decir, cubrir el vacío legal que no había sabido cubrir el derecho a la intimidad. La llamada "libertad informática" es el *derecho a controlar* el uso de los mismos datos insertos en un programa informático y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención *(habeas data)* (SSTC 11/1998, FJ 5, 94/1998[709], FJ 4). En esta sentencia, además se cuestiona, y de hecho invalida, el sistema articulado por la Ley Orgánica 15/1999, y antes por la LORTAD, para la *gestión de los ficheros públicos***.** Los efectos de la sentencia repercuten sobre los procedimientos para la comunicación o cesión de datos entre administraciones públicas y en las facultades que se conferían a estas para la denegación de los derechos de información en la recogida de datos, de acceso, de rectificación y de cancelación[710].

3.3.Recorrido histórico doctrinal y jurisprudencial sobre la privacidad estadounidense.

Como veremos a continuación, la cuestión de la privacidad no es nueva, es más, podemos decir que la historia del derecho de la protección de datos personales parte de la experiencia americana. Posiblemente la obra del Juez *Thomas MacIntrye Cooley* con la obra *"The Elements of Torts*" (1873) es la primera que cita expresamente al derecho a la intimidad o privacidad, el cual define a este derecho como *"the right to be let alone", o* derecho a ser dejado solo o no molestado. No podemos desconocer los orígenes del derecho a la intimidad y a la vida privada gracias a las aportaciones filosóficas del liberalismo -con autores como *J. Locke* o *John Stuart Mill*[711]- los cuales afirmaban que la libertad y autonomía podría ser el sustento del fin del poder absoluto. La idea de la libertad individual y del derecho a la intimidad no dejaba de ser una libertad negativa o

---

[709] Por el que se desarrollo el artículo 18.4 de la Constitución: "…Asimismo, otorga una tutela reforzada a los *datos sensibles* (como son los datos de la salud); (…) *tales datos sólo podrán ser objeto de tratamiento automatizado con consentimiento expreso y por escrito del afectado…* (apartados 1 y 2 del art. 7) (FJ 4)".

[710] Es de mencionar la STC 202/1999, de 8 de noviembre, que otorgó el amparo solicitado por el trabajador frente a sentencias de la jurisdicción social que le habían denegado la cancelación de sus datos médicos contenidos en un *fichero informatizado sobre bajas por incapacidad temporal* de su empresa ("absentismo con baja médica"). Se trata de la primera Sentencia del Tribunal sobre el *"derecho al olvido",* que, sin denominarlo así, apreció la vulneración del derecho a la intimidad del trabajador.

[711] STUART MILL, John, "*On Liberty. Prefaces to liberty*", Beacon Press, Boston, 1959.

un *status libertatis*[712]. Pero es con el caso *Warren-Brandeis* cuando se puede decir que se alcanza un reconocimiento doctrinal el derecho a "ser dejado solo".

A.) Caso Warren-Brandeis.

El abogado *Brandeis* intercambió opiniones respecto al derecho a la *privacy* y escribió el conocido artículo[713] *"right to privacy"* (1890) a través del cual se pretendía establecer la existencia de límites jurídicos que vedaran legítimamente las intrusiones sensacionalistas de la época que habían perjudicado a Warren. En dicho artículo se afirmaría que existen derechos dentro del principio de propiedad privada, considerando al derecho a la privacidad el principio de que debe aplicarse a las aspiraciones individuales, emociones y otros productos del intelecto humano. Esto posibilitaría la reclamación ante tribunales por medio del derecho general a la *"privacy"* incluso aunque se tratara de bienes inmateriales como eran los pensamientos, las emociones y la sensaciones de una persona física. Ellos entendían que cuando la información sobre la vida privada d una persona era conocida por terceros sin el consentimiento del titula, se producía el menoscabo del núcleo de la personalidad individual. Con el caso *Warren-Brandeis*, el derecho de la privacidad pierde su vertiente más "patrimonial" para consagrarse como el derecho que posee cada persona para defenderse de intrusiones ajenas (CLIMACO, 2012, 17)[714]. El concepto original del derecho a la privacidad refleja así una dimensión psicológica; *"(...) el principio que ampara los escritos personales, y toda otra obra personal, no ya contra el robo o la apropiación física, sino contra cualquier forma de publicación, no es en realidad el principio de la propiedad privada,*

[712] En el 1890, un comentarista social publicó en uno de sus artículos que "(…) la privacidad es un producto moderno, uno de los lujos de la civilización, el cual no solo pasaba desapercibido, sino que era desconocido en las sociedades primitivas (…)";"(…) mientras que la comunicación fue solamente oral se divulgaban los hechos únicamente de persona a persona, sobre un área pequeña y eran divulgados solamente en el círculo inmediato de conocidos (…)"; "(…) mientras que ahora la *comunicación* acerca *de la privacidad es impresa*, y fabrica una víctima con todos los defectos, mismos que son conocidos cientos de miles de millas de su lugar de origen*, llevando la información con todos los detalles de una persona*. Como se puede ver ya se empezaba a despertar cierta preocupación por la posible invasión ilegítima a través de la *prensa de la época*.
Ver en ADAMS ELBRIDGE, L., "The Right to Privacy and its Relation to the Law of Libel", 39 *American Law Review,* 37, Enero-Febrero 1905, pp 37–58.

[713] WARREN Samuel y BRANDEIS Louis, "The Right to Privacy", en *The Harvard Law Review*, No, 4, Boston, Harvard University, 1980. pp. 180 y ss., Edit. Civitas, edición a cargo de Benigno Pendás y Pilar Baselga, primera edición, Madrid, 1995, pp 22. Ver disponible en : http://www.law.louisville.edu/library/collections/brandeis/node/225

[714] CLIMACO VALIENTE, Ernesto (2012) Tesina "Géneis histórica-normativa del derecho a la protección de los datos personales desde el derecho comparado a propósito de su fundamento" (Pag. 17)

sino el de la inviolabilidad de la persona" (GARRIGA, 2004, 19) [715]. Brandeis, "se adelantó a la época que estaba por venir*",* ya que era consciente de los riesgos que acarrarían las *nuevas tecnologías* a la vidas privada en pleno siglo XIX. Pasados los años, *Brandeis* se convierte en magistrado y escribió un famoso y conocido voto disidente en el caso *Olmstead vs. United States*[716] decisivo para la interpretación posterior de la cuarta enmienda de la Constitución de ese país, referente sobre el que giraba el derecho de *"privacy"*.

B.) Caso Whalen vs Roe.

Resultó ser un caso muy importante para el *ámbito de la salud* en el 1977. La cuestión se centraba en la constitucionalidad de la legislación neoyorkina que requería a las autoridades competentes los nombres y dirección de pacientes que recibían prescripciones facultativas de drogas con fines médicos, como el opio y sus derivados con el objeto de incluir dicha información en una base informatizada. La Corte suprema finalmente, aunque declaró que era legítimo ejercer el poder policial estatal, reafirmó el derecho de la persona a mantener la reserva de su información personal. Es más, señalaron que la "zona de privacidad" protegida por la libertad sustantiva (XIV enmienda) no sólo amparaba la autonomía individual en la *toma de decisiones importantes* sino también el "interés" individual en evitar la revelación de asuntos personales. En concreto, la Corte Suprema afirmó: "… Somos conscientes de la amenaza para la privacidad implícita en la acumulación de *gran cantidad de información personal en los bancos de datos informatizados* y en otros enormes *archivos del gobierno*. (…) El derecho a recopilar y usar tal tipo de datos con propósitos públicos está normalmente acompañado de una correspondiente obligación estatutaria o administrativa de evitar revelaciones injustificadas"[717].

---

[715] GARRIGA DOMÍNGUEZ, Ana, *"Tratamiento de Datos Personales y Derechos Fundamentales"*, Editorial Dykinson, Madrid, 2004, página 19.

[716] La cuestión tenía que ver con determinar si las escuchas telefónicas vulneraban el derecho a la privacidad, toda vez que pudieran considerarse como "requisas y registros irrazonables". La mayoría de la Corte optó por una interpretación literalista –dado que entendían que se interceptaban voces fuera de las casas de las personas- por el contrario, *Brandeis* reindivicó por medio del voto disidente una interpretación más dinámica y abierta que se adapta al *cambio tecnólogico* que estaba por llegar. *Brandeis* afirmaba que la interceptación de comunicaciones por cable podía invadir la privacidad más peligrosamente que la interceptación por correspondencia. En definitiva, a cuarta enmienda según él, no protegía el derecho de propiedad sino el derecho a ser dejado solo.

[717] Sentencia del Tribunal Supremo de los EEUU Whalen v. Roe (1977) 429. U.S. 589, sobre protección de datos persobales. Traducido por E. Guillén López. Recuperado de: http://www.ugr.es/~redce/REDCE7/articulos/16sentenciasupremoamericano.htm

4. LA IMPORTANCIA DEL DERECHO DE PROTECCIÓN DE DATOS DE SALUD DIGITAL EN LA ERA TECNOLÓGICA.

"...las personas necesitan tener la tutela de su cuerpo electrónico"

(Stefano Rodotà)

La enfermedad a lo largo de la historia se ha traducido en muchas ocasiones como sinónimo de "estigma social, castigo divino y fruto del pecado personal o familiar", presentándose de una forma en la que su exposición pública dañaría irreparablemente la consideración social, la imagen y la dignidad de cualquier persona. No parece por tanto necesario convencer de que el indebido acceso a datos reveladores de enfermedades o padecimientos puede, no solo afectar a la intimidad, sino limitar seriamente el ejercicio de otros derechos y libertades fundamentales, como el derecho de protección de datos. Esta situación estigmatizante se extiende hasta nuestros días en plena revolución tecnológica del 5G, de la era de Blockchain, de las Smart Cities, de la IoTH, etc.

Los *datos personales de salud* se entienden cada vez más como claves para la sostenibilidad de los sistemas de salud públicos y privados en el marco de la Sociedad de la Información. Un mejor acceso y conocimiento de los datos de salud y bienestar posibilitado por la tecnología, conduce al empoderamiento de las personas al darles la capacidad de tomar decisiones sobre sus propios datos, así como a desempeñar un papel activo en la gestión de su bienestar y sus condiciones de salud[718].

La *identidad digital* ha traído como resultado que la persona y la intimidad ya no sólo se vean amenazadas en el mundo "real" sino que también puedan serlo en el mundo "virtual". El usuario de Internet pasa una media de dos horas al día solo en las redes sociales[719] y a lo largo de su vida pasará hasta seis años y no sólo eso, el almacenamiento de datos digitales no dejará de experimentar un crecimiento sin antecedentes en la historia 720., donde el 90% de los datos del mundo se crearon en los últimos dos años.

[718] Vid https://d-lab.tech/challenge-2/
[719] Vid https://www.statista.com/statistics/433871/daily-social-media-usage-worldwide/
[720] Vid https://www.eetimes.com/author.asp?section_id=36&doc_id=1330462

El profesor *Stefano Rodotà* (2003) ya declaraba hace varios años que nuestro cuerpo era una fuente abierta y continua para extraer datos; "el entrelazamiento de electrónica, biología y genética ya ha abierto nuevos escenarios, tanto prometedores como inquietantes". Este autor relacionaba a nuestro cuerpo humano como si se tratara de una "contraseña"[721] pero que no sólo servían para identificar o como claves sino también para clasificar. Esos datos a los que se refiere el profesor a las huellas dactilares, a la geometría de la mano o de los dedos o de las orejas, al iris, a la retina, a los rasgos, a los olores, a la voz, a la firma, a la utilización de un teclado, a la manera de andar, al ADN. RODOTÀ[722] se refería a la evolución de ;

Es decir, pasamos del control de nuestros datos personales (autodeterminación informativa) convencional al control de nuestro cuerpo ("físico" y "electrónico[723]"). Cualquier tratamiento de datos biométricos, por ejemplo, deberá ser juzgado en referencia al cuerpo entero.

El 30 de mayo de 2017, se celebró el primer *Conversatorio sobre Derechos Digitales de los Ciudadanos*[724] organizado por la Secretaría del Estado para la Sociedad de la Información y Agenda Digital (D. Jose María Lassalle Ruíz), al que tuve el privilegio de acudir[725], se trataron cuestiones de gran interés como si ¿Existen nuevos derechos ligados a la vida digital o son una traslación de los derechos fundamentales al ámbito online? ¿Cuáles son los mecanismos con los que cuenta el Derecho para su protección?, desafíos sobre los avances tecnológicos, globalización y democracia, etc., entre otros. Los Estados Miembros de la Unión Europea en el proceso de adaptación de la norma europea a las legislaciones nacionales, han ido creando declaraciones de

[721] Vid https://www.punto-informatico.it/rodot-il-corpo-umano-una-password/
[722] Vid. Il nuovo habeas corpus e Il corpo giuridificato, in Trattato di biodiritto (2010). Pp. 3-60, 354-5
[723] Vid. http://www.privacy.it/archivio/rodo20040916.html
[724] En este conversatorio esta previsto que pudiera acudir Stefano Rodotà pero lamentablemente no pudo acudir. En su memoria se redactó la que iba a ser su ponencia disponible en: https://www.red.es/redes/es/sala-prensa/recursos-multimedia/pdfs/ponencia-de-stefano-rodot%C3%A0-para-el-conversatorio-sobre-derechos. Gracias a él, todos los académicos que nos apasiona el ámbito de los derechos digitales tenemos un gran legado que continuar todos los académicos que nos apasiona el los derechos digitales y los derechos fundamentales de las personas y ciudadanos.
[725] Mi más sincero agradecimiento a mi estimado mentor D. Ricard Martínez Martínez por la invitación.

derechos de internet como en el caso de Italia[726] o han incorporado esas declaraciones con carácter vinculante en el cuerpo de una norma de desarrollo del derecho fundamental, como es el caso de España con la LOPDGDD aprobado el 5 de diciembre de 2018 [727].

[726]Vid. http://www.camera.it/application/xmanager/projects/leg17/commissione_internet/dichiarazione_dei_diritti_internet_pubblicata.pdf

[727] Sin ir más lejos, en nuestro país, se ha apostado firmemente por los derechos digitales de la ciudadanía que desde el Colegio de Abogados de Barcelona y al mando de los prestigiosos expertos juristas *D. Rodolfo Tesone y D. Francisco Bonatti*, se presentó la *Carta de Barcelona por los derechos de la ciudadanía en la era digital*, el 21 de ferbrero de 2019, en el marco del Worl Mobile Congress (II Digital Law World Congress).

CAPÍTULO VII. CUESTIONES PREVIAS Y EL NUEVO RÉGIMEN JURÍDICO EN MATERIA DE PROTECCIÓN DE DATOS EN SALUD Y TECNOLOGÍA

SUMARIO: 1. FLUJO DE DATOS DE SALUD EN EL MERCADO ÚNICO DIGITAL. - 2.OPEN DATA DE SALUD.- 3.REUTILIZACIÓN DE DATOS Y LA SALUD. - 4.LOS METADATOS DE SALUD.- 5.LOS HISTORIALES MÉDICOS ELECTRÓNICOS.- 6.SALUD, TECNOLOGÍA Y EL DERECHO DE PROTECCIÓN DE DATOS.- 7.MENORES DE EDAD, SALUD, TECNOLOGÍA Y PROTECCIÓN DE DATOS.

"Lo que te preocupa, te controla".

(Locke)

1. FLUJO DE DATOS DE SALUD EN EL MERCADO ÚNICO DIGITAL

Las nuevas oportunidades derivadas del *big data* junto con el aprovechamiento de la analítica de datos, el *deep learning*[728], la *m-Health*, *w-Health*, *e-Health*, IoT, *IoTH*, o herramientas de apoyo sanitario requieren de soluciones y sistemas digitales de información que no suelen ser compatibles entre sí lo que impide el intercambio y la puesta en común dentro de un Estado y a nivel transfronterizo entre Estados Miembros. Inevitablemente se traduce en ineficiencia puesto que no se puede aprovechar ese flujo de datos y aumenta los costes de desarrollo y mantenimiento. La puesta en común de datos y sus analíticas tendrían indudablemente un enorme repercusión para ayudar a la prevención, la detección temprana y el control de enfermedades infecciosas.

Antes de la entrada en vigor del nuevo RGPD, desde la *Comisión Europea*, en 2017, se fueron planteando varias iniciativas que iban marcando el camino hacia al citado Reglamento como fueron:

[728] Vid. https://www.immedicohospitalario.es/noticia/15601/la-inteligencia-artificial-amenaza-la-privacidad-de-los-datos-de-salud

i. Mejor *acceso y reutilización* de los datos del sector público.
ii. *Intercambio de datos científicos*. Dentro de las recomendaciones se incluía, por ejemplo, la creación de una Nube Europea de Ciencia Abierta[729].
iii. *Intercambio de datos* entre empresas y empresas y empresas y gobierno.
iv. Asegurar los *datos de salud de los ciudadanos*.

Estas iniciativas se complementarían con las normas que propondría la UE sobre *el libre flujo de datos no personales en la UE*[730] presentado por la Comisión en septiembre de 2017. Estas nuevas normas junto con las existentes sobre datos personales, permitirían el almacenamiento y tratamiento de datos no personales en toda la UE y de esta manera impulsar la competitividad de las empresas europeas y la modernización de los servicios públicos en el mercado único de servicios de datos de la UE. Y es que eliminar las restricciones de localización de los datos supondría el aumento del PIB en un 4%. Básicamente las normas se basarían en:

i. Que los EEMM *no* pueden *obligar a las empresas a ubicar su almacenamiento* o tratamiento *dentro de sus fronteras*. Eliminar ese "obstáculo" hará que las empresas no tengan que duplicar sus sistemas de TI o guardar los mismos datos en diferentes países.
ii. El principio de la disponibilidad de datos para el *control reglamentario*.
iii. Se desarrollarán *códigos de conducta* de la UE para eliminar obstáculos para cambiar entre proveedores *cloud* y portar los datos.

Por su parte, la *Comunicación sobre la transformación digital de la salud y la atención en el mercado único digital*[731] de la Comisión Europea (2018) identificó tres prioridades:

i. *El acceso seguro de los ciudadanos a sus datos de salud*, también a través de las fronteras, permite a los ciudadanos acceder a sus datos de salud en toda la UE.

[729] Comisión Europea (20 de noviembre 2018). Nube Europea de Ciencia Abierta (EOSC). Recuperado de https://ec.europa.eu/research/openscience/index.cfm?pg=open-science-cloud
[730] Comisión Europea (13 de septiembre 2017). Com (2017) 495 Final. Proposal for a Regulation of the European Parliament and of the council on a framework for the free flow of non-personal data in the European Union http://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-495-F1-EN-MAIN-PART-1.PDF
[731] Comisión Europea (25 de abril 2018). Comunicación sobre la habilitación de la transformación digital de la salud y la atención en el mercado único digital. Empoderar a los ciudadanos y construir una sociedad más sana. Recuperado de https://ec.europa.eu/digital-single-market/en/news/communication-enabling-digital-transformation-health-and-care-digital-single-market-empowering

ii. Medicina personalizada a través de una *infraestructura de datos europea compartida*, que permite a los investigadores y otros profesionales aunar recursos en toda la UE.

iii. *El empoderamiento de los ciudadanos* con herramientas digitales para la retroalimentación del usuario y la atención centrada en la persona.

Pero además es de resaltar lo siguiente:

i. Se pretende alentar a las *autoridades nacionales y otras partes interesadas*, en particular a los *investigadores*, a compartir datos e infraestructura. Uno de los objetivos iniciales es proporcionar acceso a al menos 1 millón de genomas secuenciados en la Unión Europea para 2022.

ii. La Comisión elaboraría un catálogo de especificaciones técnicas comunes para respaldar el *acceso transfronterizo seguro* a datos genómicos y otros datos de salud con fines de investigación

iii. La Comisión implementaría *proyectos piloto* basados en *datos del mundo real* (datos después de *ensayos clínicos*[732], datos recopilados de pacientes reales después de que los medicamentos o productos se hayan lanzado al mercado) para satisfacer las necesidades de los pacientes con medicamentos o terapias. Por ejemplo, comenzando con las *enfermedades raras*.

2. OPEN DATA DE SALUD

Al no existir iniciativas reales (al menos en nuestro país de asistencia sanitaria) donde se puedan compartir datos de pacientes y que puedan ser utilizados en el ámbito investigador o clínico debido al "principal problema de la privacidad" (Claerhout & DeMoor[733], 2005; B. Malin, Karp, & Scheuermann, 2010[734]), deriva en una "gran carencia de datos públicos que puedan ser utilizados en entornos de investigación". Y en

[732] SEPD (2019). Opinion 3/2019 sobre las preguntas y respuestas sobre la interacción en el Reglamento de ensayos clínicos (CTR) y el RGPD. Recuperado de https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-32019-concerning-questions-and-answers-interplay_en

[733] Claerhout, B., & DeMoor, G. J. E. (2005). Privacy protection for clinical and genomic data: The use of privacyenhancing techniques in medicine. *International Journal of Medical Informatics*, 74(2–4), 257–265. Recuperado de http://doi.org/10.1016/j.ijmedinf.2004.03.008

[734] Malin, B., Karp, D., & Scheuermann, R. H. (2010). Technical and Policy Approaches to Balancing Patient Privacy and Data Sharing in Clinical and Translational Research. *Journal of Investigative Medicine* : The Official Publication of the American Federation for Clinical Research, 58(1), 11–18. Recuperado de http://doi.org/10.231/JIM.0b013e3181c9b2ea

este contexto es donde las iniciativas de datos abiertos posibilitan la utilización y redistribución de los datos por parte de cualquier usuario de forma libre con la única restricción, como máximo, de garantizar la autoría de las fuentes o autores de los datos[735].

Si hablamos en términos generales, España es el segundo país europeo más preparado para el uso de *open data* y así lo refleja el *"Informe de Madurez 2018 de los Datos Abiertos"*[736], publicado por el Portal Europeo de Datos Públicos. Por su parte el open data en el ámbito de la salud tiene debilidades jurídicas en materia de protección de datos aunque también grandes bondades. Por ejemplo, esos beneficios tienen que ver con el aumento de la eficiencia del sistema, la reducción de costes, el incremento de la transparencia en gestión pública que se traduce en una mayor implicación y empoderamiento del paciente, y repercutiría en una mejora del sistema sanitario. Y es en este sector donde se genera gran cantidad de datos (proveniente de muchas fuentes y actores). Y es que como se sabe obtener datos de salud no es nada fácil ni barato y el open data puede facilitar el contexto actual mejorando la rentabilidad, eficiencia y atrayendo la innovación e investigación. En concreto, en nuestro país, los datos de salud se concentran principalmente en las *administraciones públicas* como prestadores de asistencia sanitaria aunque cada vez se genera mayor información por un lado, por proveedores de la salud como es la *industria farmacéutica* y por el otro, el sector tecnológico en el que se incluyen los dispositivos móviles con apps de *mHealth*[737] *y wearables*. Aunque como veremos el mayor obstáculo se encuentra en que la información no es del todo estructurada y hace que aún no está del todo maduro este sector.

Por otro lado, en España no existe un directorio específico de naturaleza sanitaria y el portal de datos del gobierno de España es un directorio genérico sobre

[735] Por ejemplo, *Linked Open Data Cloud* (LODC), permite la interconexión de datasets de diferente índole utilizando como enfoque tecnológico de representación y enlazado de datos Linked Data. En el informe se señala que "es imprescindible mencionar la importancia y la utilización actual de Open Data en el ámbito sanitario (Open Health Data) tal y como indica la figura X (James Manyika et al., 2013) ya que la utilización abierta de datos sanitarios puede ayudar en prácticamente todos los sectores del ámbito sanitario".

[736] European Data Portal (2018) Open Data Maturity in Europe. Recuperado de https://www.europeandataportal.eu/sites/default/files/edp_landscaping_insight_report_n4_2018.pdf

[737] SEPD (21 de mayo de 2015). Opinion 1/2015. Mobile Health. Reconciling technological innovation with data protection. Recuperado de https://edps.europa.eu/sites/edp/files/publication/15-05-21_mhealth_en_0.pdf

datos abiertos que abarca un espectro más generalista. Se trata de un camino lleno de obstáculos. Algunos de los obstáculos tienen que ver (Andreu, 2017): (i) En relación con las *barreras institucionales, burocráticas y culturales* a la apertura de datos; (ii) en relación con la *protección de la privacidad* y la desconfianza hacia un uso incorrecto de estos datos que pueda ser perjudicial; (iii) en relación con la *necesidad de un "buen análisis" de esos datos; (iv) e*n relación con los con los *estándares técnicos y la interoperabilidad*.

El portal de Transparencia del Instituto Nacional de Estadística[738], es un ejemplo de open data o la *iniciativa Aporta* y que está destinada a promocionar la cultura de apertura de información e incorpora una sección dedicada a la salud (http://datos .gob.es/es/catalogo). Las Comunidades Autónomas tienen también portales de open data como el gobierno catalán[739] con posibilidad de descargar en varios formatos.

En Europa, por ejemplo, el *European Core Health Indicators* (ECHI)[740] de la Comisión Europea, tiene el objetivo de proporcionar información de salud y un sistema de conocimiento comparables para monitorear la salud a nivel de la UE. Estos indicadores permiten establecer comparaciones (ej. comparar indicadores de salud en relación con la mortalidad infantil con factores demográficos, como la población y la tasa de nacimiento para un país específico). A continuación, un ejemplo:

Titulo	**Ejemplos**
Situación demográfica y socioeconómica	Población, tasa de natalidad, desempleo total
Estado de salud	Mortalidad infantil, VIH/sida, accidentes de tráfico
Determinantes de la salud	Fumadores habituales, consumo/disponible. de fruta.
Intervenciones en salud, servicios de salud	Vacunas niños, camas hospital, gasto sanitario
Intervenciones en salud, promoción de salud	Políticas sobre nutrición saludable

Tabla 43. Tabla ejemplos indicadores de salud. Fuente: Comisión Europea (texto). ECHI.

[738] Vid. http://transparencia.gob.es/servicios-buscador/buscar.htm?categoria=estadistica&ente=E04921901&historico=false&lang=es

[739] Vid. https://analisi.transparenciacatalunya.cat/browse?tags=salut

[740] Comisión Europea (Agosto 2013) Evaluation of the use and impact of the European Community Health Indicators ECHI by Member States. Final Report. Recuperado de https://ec.europa.eu/health/sites/health/files/indicators/docs/echi_report_v20131031.pdf

Además, la Comisión también proporciona una herramienta (aún por mejorar) para explotar estos datos (*EHCI data tool*)[741], la cual permite crear gráficos y realizar cálculos con la información. No obstante, queda mucho para que "esta información se convierta en productos de valor añadido para el ciudadano"(Andreu, 2017)[742].

A nivel nacional el país más avanzado en esta materia es el Reino Unido, con el portal de datos del Servicio público de salud (NHS)' el cual no solo presenta datos e indicadores estadísticos, sino también valoraciones de cada centro sanitario, coste de tratamiento, resultados de tratamientos clínicos, incidencia de enfermedades, etc. En el documento elaborado por el gobierno inglés *"The open data era in health and social care"* (2014)[743] se pueden extraer algunas conclusiones (algunas que ya hemos adelantado); acceso de la ciudadanía a la información sobre servicios que se adapten mejor a su salud, información de proveedores de salud y tratamiento, etc. Ello se traduce en rentabilidad y compatibilidad posibilitando en general, el crecimiento económicos, y en particular, mejora de la atención sanitaria e innovación y atrae la investigación biomédica. No obstante, habrá que ser cuidadosos para evitar situaciones que están ocurriendo en gobiernos extranjeros como en China, donde recientemente se encontró una base de datos abierta[744] con información privada de millones de mujeres con datos como edad, nivel educativo, estado civil, números telefónicos, ubicación, número de identidad, dirección y una columna que decía *BreedReady* (término para expresar preparada para reproducir). Aunque no está claro si la información pertenece a un servicio de citas, el gobierno o alguna empresa u organización. El hacker Víctor Gevers, que descubrió la base de datos anteriormente encontró también una base de datos que, afirma, pertenece a una compañía de vigilancia, cuyo objetivo era monitorizar a 2,5 millones de residentes en Xinjiang**.**

En definitiva, ningún dato relacionado con la salud en el registro de la unidad o a nivel de paciente/persona puede ser divulgado como Datos Abiertos. Si Se produce una

---

[741] Ibidem.

[742] Andreu Martínez, M.Belén (2017) Open Data En El Ámbito Sanitario Y Su Compatibilidad Con La Privacidad Del Paciente. Les Éditions del'IMODEV (Improving Public Policies in a Digital World). Open Journals. Revue Internationale des Gouvernements Ouverts. Vol. 5. Recuperado de http://ojs.imodev.org/index.php/RIGO/article/view/200/330

[743] Verhulst, S., Noveck, B., Caplan, R., Brown, K., Paz, C. (mayo 2014). The open data Era in Health and Social Care. GOBLAB NHS England. Recuperado de www.thegovlab.org/static/files/publications/nhs-full-report.pdf

[744] Kuo, L. (11 marzo 2019). La base de datos de China enumera el estado de "raza" de 1,8 millones de mujeres. The Guardian. Recuperado de https://www.theguardian.com/world/2019/mar/11/china-database-lists-breedready-status-of-18-million-women

violación a la protección de datos, aquellos que los procese y los divulgue serán responsables y deberán responder antes los afectados.

3. REUTILIZACIÓN DE DATOS Y LA SALUD.

La Comisión Europea, en su documento *"Redesigning health in Europe for 2020"* (2012), [745]define 5 recomendaciones para reorientar las políticas de salud. Precisamente, una de las recomendaciones es potenciar la reutilización de la información de salud para mejorar el acceso a esta información por parte de los investigadores, transferir los resultados de la investigación a la práctica clínica, crear una cultura de transparencia y mejorar los servicios sanitarios favoreciendo el *benchmark*[746] entre centros sanitarios.

Como señala el jefe de la Agencia de calidad, *Ramon Maspons*[747], y evaluación sanitaria de Cataluña[748] (AQuAS), ésta "desarrolló un proyecto dirigido a la comunidad científica poniendo a su disposición información relacionada, anonimizada y segura del sistema sanitario catalán con el objetivo de facilitar la investigación la innovación y la evaluación". Además señalaba que solo daría respuesta a las solicitudes que tuvieran finalidades de investigación biomédica y evaluación del propio sistema sanitario realizando anonimización y se denominaría *VISC+*[749].

[745] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=2650

[746] Según wikipedia, se trata de "la evaluación comparativa es la práctica de comparar los procesos de negocios y las métricas de rendimiento con las mejores y mejores prácticas de la industria de otras compañías. Las dimensiones típicamente medidas son calidad, tiempo y costo".

[747] Agència de Qualitat i Avaluació Sanitàries de Catalunya – Generalitat de Catalunya. Dep. de Salut. Reutilización de la información para mejorar la investigación y la evaluación de los servicios sanitarios. Recuperado de www.fundacio.udl.cat/biobancos/doc/sesiones/Sesion4-RamonMaspons.pdf

[748] Según *Maspons,* Cataluña fue propicia dado el sistema sanitario y sus sistemas de información consolidados, gracias a la información generada de calidad y tiene profundidad histórica, a la red de excelencia de universidades, hospitales y centros de investigación del ámbito básico, clínico y epidemiológico, a la industria catalana del ámbito de las ciencias de la vida es potente (farmacéutica, biotecnológica, etc.) y a experiencias previas como el SIDIAP".

[749] Otros ejemplos de proyectos son care.data (que no han tenido el resultado que se deseaba) (Reino Unido) o Pharmo (Holanda) o PCORnet (EUA). Por ejemplo, BIFAP es una iniciativa que fue presentada en 2015 que consistía en una base de datos informatizada de registros médicos de atención primaria para la realización de estudios fármaco-lógicos, que pertenece a la AEMPS. O la SIDIAP (antecesora de VISC+) fundada en el 2010 para promover la investigación basada en los datos clínicos de primaria y otras bases de datos complementarias.

Las bases de datos provenían de las siguientes fuentes de información según la AQuAS:

Imagen 67. Fuentes de información AQuAS. Fuente: AQuAS. Generalitat de Catalunya

A pesar de tratarse VISC+ de un proyecto pionero y prometedor, aparecieron algunas controversias respecto a la reutilización de datos y finalmente fue paralizado y sustituido por el programa "Padris".

Pero como ya adelantábamos; la anonimización no puede garantizar siempre la absoluta reidentificación puesto que se puede dar que se produzca una anonimización "reversible" y esto facilite la reidentificación todo ello unido al riesgo ético-legal de la discriminación por el profling que van asociados a esta tipología de proyectos, desembocaría en un resultado no deseable para los titulares de datos personales. No solo es imprescindible que las medidas sean las más adecuadas sino también la propia toma correcta de decisiones en los procesos de gestión de datos, la transparencia por parte de los actores y participantes (pacientes y profesionales) y la propia confianza. A continuación, hablemos de algunas cuestiones referentes al *marco jurídico* a tener en cuenta. En primer lugar conviene tener presente, el documento *"Orientaciones sobre protección de datos en la reutilización de la información del sector público"*[750] de la AEPD donde se reúnen aquellos aspectos a tener en cuenta por el sector público a la hora de abrir sus datos de forma compatible con la garantía del *derecho fundamental a la protección de datos*. La reutilización de datos puede realizarse en entornos de *big*

[750] Unión Europea (2012). eHealth Task Force Report. Redesigning health in Europe for 2020. https://datos.gob.es/es/documentacion/orientaciones-sobre-la-proteccion-de-datos-en-la-reutilizacion-de-la-informacion-del

data o de minería de datos y esto genera cierta preocupación acerca de la vulneración de la privacidad; preocupación que debería ser superada al ponderarla con los beneficios innegables que puede proporcionar a la sociedad. Por ello, según la AEPD, la existencia de estos riesgos no debe excluir la posibilidad de reutilizar la información pública, acción impulsada y motivada por el legislador europeo, que en todo caso, se implementarán garantías jurídicas adicionales a las medidas técnicas y organizativas. No se puede olvidar el contexto dinámico y volátil de las TIC en el que se desarrolla esta acción y en donde debe producirse la protección de los derechos y libertades de las personas al igual que el propio valor económico de la información. En dicha guía, se tiene muy presente la importancia de medidas como la *evaluación de impacto de la reutilización en la protección de datos personales (EIPD*) y soluciones de soluciones proactivas como la *anonimización* de los datos. Además, algo importante a señalar, en el texto se explica cómo realizar la anonimización a través de **c**ompromisos jurídicamente vinculantes como la *indicación expresa de prohibir la reidentificación y reutilización* de los datos personales en la toma de decisiones, o algunas medidas de ejemplo para asegurar el cumplimiento de dichas garantías jurídicas que van desde las *evaluaciones periódicas sobre el riesgo de reidentificación* hasta la realización de *auditorías* sobre el uso de la información reutilizada o la inclusión de *advertencias* en los sitios web sobre la reidentificación (como realizan centros sanitarios que realizan investigación biomédica) o medidas coercitivas, como las penalizaciones económicas o la posibilidad de suspender o impedir la reutilización de documentos. Habida cuenta las dificultades que puede conllevar esta tarea para algunas Administraciones públicas, la AEPD prevé que el reutilizador pueda colaborar con la Administración en cuestión y que pueda llevar a cabo su propia evaluación de impacto o riesgos de reidentificación una vez obtenida la información.

En segundo lugar, pero también es importante otro documento de la AEPD, en este caso de las "Orientaciones y garantías en los procedimientos de anonimización de datos personales"[751]. En el cual "se establecen de forma detallada los principios de anonimización, las fases del procedimiento (con la definición del equipo de trabajo, la evaluación de riesgos, la viabilidad del proceso, definición/eliminación /reducción de variables de identificación, la selección de la técnica de anonimización…), la formación

[751] Vid. https://datos.gob.es/es/documentacion/orientaciones-y-garantias-en-los-procedimientos-de-anonimizacion-de-datos-personales

e información al personal implicado, las garantías, auditorías del proceso, etc." (ANDREU, 2017). Esta autora recalca algo que se señala en dicho documento y que el lector ya sabrá o empezará a asimilar: "no es posible garantizar al 100% el anonimato absoluto (sobre todo a lo largo del tiempo)". Y como ella declara acertadamente, "la fortaleza de la anonimización habrá que sustentarla en medidas de muy diverso tipo: evaluaciones de impacto, organizativas, de seguridad, tecnológicas y en cualquier otra que permita atenuar los riesgos y paliar las consecuencias en el caso de que estos se materialicen".

En tercer lugar, no podemos pasar por alto a la Ley 18/2015, de 9 de julio, por la que se modifica la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público[752], que establece que las Administraciones y los organismos públicos tienen la *obligación inequívoca de autorizar la reutilización* de su información. Conviene destacar los siguientes aspectos por cuanto nos interesa; (i) se amplía el ámbito de aplicación a las bibliotecas (incluidas las universitarias) dado el importante volumen de recursos de información y los proyectos de digitalización; (ii) se promociona el uso, siempre que sea posible y adecuado, ofrecerlos en formatos abiertos (que garantice la interoperabilidad) y legibles por máquina junto con sus metadatos; (iii) la ley incorpora la obligación de fomentar el uso de licencias abiertas, de tal forma que las licencias para la reutilización de la información del sector público planteen las mínimas restricciones posibles.

En cuarto lugar, y más reciente, tenemos que mencionar de la Ley Orgánica 3/2018, de 5 de diciembre de protección de datos y garantía de derechos digitales. En concreto a la Disposición transitoria sexta que regula la reutilización con fines de investigación en materia de salud y biomédica de datos personales:

> "Se considerará lícita y compatible la reutilización con fines de investigación en salud y biomédica de datos personales recogidos lícitamente con anterioridad a la entrada en vigor de esta ley orgánica cuando concurra alguna de las circunstancias siguientes:
>
> a) Que dichos datos personales se utilicen para la *finalidad concreta* para la que se hubiera prestado consentimiento.

[752] BOE. Ley 18/2015, de 9 de julio , por la que se modifica la reutilización de la información del sector público. Recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-7731

b) Que, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen tales datos para *finalidades o áreas de investigación relacionadas con la especialidad médica o investigadora* en la que se integrase científicamente el estudio inicial".

Esta disposición despertó controversias en el momento de su tramitación parlamentaria por parte del sector sanitario e instituciones como la Sociedad Española de Oncología Médica (SEOM)[753] que ven como puede poner en peligro la investigación biomédica al no autorizar la reutilización de datos ni la prestación de consentimiento *para otros fines* que no fueron los previstos inicialmente. Se quejan de que no se haya tomado en consideración que la investigación médica es una actividad de interés público general.

Visto el marco jurídico y regulatorio en el que se puede encuadrar la investigación biomédica en entornos de big data, expondré algunas cuestiones de interés según mi parecer. Llegados a este punto, podemos plantearnos si será posible avanzar y evolucionar en relación con la apertura de datos con base en la Ley de transparencia[754] hacia un *"auténtico open data"* (Mateu, 2017) y por ejemplo, se ponga a disposición de los usuarios ficheros como historiales clínicos electrónicos (como hace el NHS inglés o el gobierno francés) o prestaciones farmacéuticas dirigidos, pero dirigidos en principio a la investigación biomédica y a la innovación en pro del sistema de salud (privado y público). Pero hay algo obvio y es que no sería disponible esta reutilización para todos, sino sólo para centros sanitarios y de investigación quedando al margen la industria farmacéutica o aseguradora. Sobre ello, hablaremos largo y tendido a lo largo de este trabajo.

En Finlandia[755], se aprobó recientemente una ley que regula las transferencias de datos personales, sociales y de salud, de los responsables de datos del propósito principal de tratamiento a un ecosistema formado por administradores de los principales registros nacionales como el Institución del Seguro Social, el Centro de Registro de la Población, la Oficina de Estadística de Finlandia y el Centro de Seguridad de Pensiones,

[753] RedacciónMédica (12 de febrero de 2018). "La LOPD obvia el papel del Comité de Ética en la investigación oncológica". Recuperado de https://www.redaccionmedica.com/secciones/oncologia-medica/-la-lopd-obvia-el-papel-del-comite-de-etica-en-la-investigacion-oncologica--6934

[754] BOE, Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887

[755] Vid. https://blogs.dlapiper.com/privacymatters/finland-parliament-approves-new-act-on-the-secondary-use-of-social-and-health-care-personal-data/

Autoridad Nacional de Supervisión para la Salud y el Bienestar, Instituto Finlandés de Salud Ocupacional y Agencia de Medicamentos de Finlandia. El uso secundario de datos personales almacenados en los registros de los controladores de datos mencionados anteriormente se permitirá con fines permitidos bajo una *licencia revocable de plazo fijo*. Las decisiones sobre licencias están sujetas a apelación. La autoridad de la licencia será una nueva *'ventanilla única'* que opera bajo la supervisión del Ministerio de Asuntos Sociales y Salud de este país. Esta licencia se puede aplicar para actividades educativas, de gestión de la información, así como para actividades de innovación y desarrollo que vayan más allá de los propósitos tradicionales de *investigación* reflejados en el artículo 89 del RGPD. Me pregunto; ¿se extenderá este modelo al resto de los países europeos? ¿Será una cuestión más bien cultural?

Concluyendo, me gustaría resaltar la conclusión de la profesora Mateu, que dice; "nos encontramos, así, con la paradoja de que el empoderamiento del individuo pasa desde luego por una información de calidad, pero al mismo tiempo se disminuyen sus facultades de controlar el uso que se hace de su información sanitaria. Está por ver que las garantías que se disponen para proteger la información sean suficientes para evitar un uso con fines comerciales u otros no deseados. Desde mi punto de vista, no solo el problema se focaliza en si las medidas técnicas y organizativas (sobre todo las referentes a la anonimización) serán suficientes para garantizar el derecho fundamental, sino que haciendo eco de las alertas del sector sanitario se pueda aletargar el impulso y desarrollo de la investigación e innovación frenado por exceso de trabas burocráticas y legales. Posiblemente no es precipitado adelantar alguna solución técnica, a las alturas de este trabajo. Me atreveré a vaticinar que los sistemas DLT/Blockchain aplicados al sector sanitario y de la industria del cuidado de la salud podrían llegar a aportar su parte de solución.

4. LOS METADATOS DE SALUD

Podemos servirnos de la definición de la propuesta del Reglamento sobre la privacidad y las comunicaciones electrónicas[756] (Comisión Europea, 2017, 29) para entender a priori el alcance que supondría en nuestro ámbito:

[756] COMISIÓN EUROPEA. Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la

> Los "metadatos de comunicaciones electrónicas son datos tratados en una red de comunicaciones electrónicas con el fin de transmitir, distribuir o intercambiar contenido de comunicaciones electrónicas; se incluyen los datos utilizados para rastrear e identificar el origen y el destino de una comunicación, los datos sobre la ubicación del dispositivo generados en el contexto de la prestación de servicios de comunicaciones electrónicas, así como la fecha, la hora, la duración y el tipo de comunicación";

Sin duda, los metadatos son importantes[757]. Los metadatos facilitan a los proveedores de comunicaciones electrónicas información acerca de comportamientos individuales privados como llamadas a líneas de prevención de suicidios realizada desde un puente o los proveedores pueden tener información acerca de la recepción de un correo electrónico de un laboratorio con los resultados del análisis de VIH, que a continuación se realizó una llamada a profesionales sanitarios y que se consultó un foro de e-pacientes de VIH en la misma franja horaria, todo ello, sin que obviamente accedan al contenido del correo o de la conversación o que se realizó una búsqueda por internet sobre clínicas de aborto y que en esa franja horaria se realizó una llamada en la misma franja horaria a una de esas clínicas. También en tweet donde se hable del estado de salud (gripe) pueden tener decenas de metadatos y con algunos de ellos se podría identificar a alguien con un porcentaje de acierto altísimo" tal y como han demostrado algunos investigadores[758]. Además señalan que "la ofuscación de datos es difícil e ineficaz para este tipo de datos: incluso después de perturbar el 60% de los datos de formación, todavía es posible clasificar con una precisión superior al 95%" (sobre todo aplicada a redes sociales como Twitter). Esto es absolutamente relevante.

Estos autores señalan que "sorprendentemente, los metadatos a menudo se siguen clasificando como no sensibles y de hecho, en el pasado, los investigadores y los profesionales se han centrado principalmente en el problema de la identificación de un usuario a partir del contenido de un mensaje" (PEREZ et al. 2018).

---

privacidad y las comunicaciones electrónicas) (2018). Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017PC0010&from=LV

[757] Vid. https://ssd.eff.org/es/module/por-qu%C3%A9-los-metadatos-son-importantes

[758] Perez , B., Musolesi, M., Stringhini, G. *You are your Metadata: Identification and Obfuscation of Social Media Users using Metadata Information*. University College London. Recuperado de https://www.ucl.ac.uk/~ucfamus/papers/icwsm18.pdf

El desarrollador australiano *Simon Elvery*[759] (2018), realizó una investigación *("datalife")* en la cual interceptó y grabó cada bit de datos enviados desde su teléfono y ordenador. En una semana se realizaron 300.000 solicitudes o lo que es lo mismo, una cada segundo de media[760]. Los usuarios desconocemos qué finalidades existen y a quien se envían y es que aunque no sean datos visibles se tratan de información de carácter personal y privado.

Si volvemos al marco jurídico, encontramos que la Comisión Europea siguió esa línea interpretativa y así lo declara :"según el TJUE, los metadatos derivados de las comunicaciones electrónicas pueden también revelar información muy delicada y de carácter personal, como reconoció expresamente el TJUE. La mayoría de los Estados miembros reconoce también la necesidad de que la protección de las comunicaciones constituya un derecho constitucional diferenciado"(Comisión Europea, 2017, 11). Para entenderlo mejor, el legislador señala que "entre esos metadatos figuran los números a los que se ha llamado, los *sitios web visitados, la localización geográfica o la hora, la fecha y la duración de una llamada*, información que permite extraer conclusiones precisas sobre la *vida privada de las personas participantes* en la comunicación electrónica tales como sus relaciones sociales, sus costumbres y actividades de la vida cotidiana, sus intereses, sus preferencias, etc." (pp 14). El futuro Reglamento exigirá "a los proveedores de servicios de comunicaciones electrónicas que obtengan *el consentimiento* de los usuarios finales para tratar metadatos de comunicaciones electrónicas(…)" (pp 18).

Ahora bien, a mi modo de ver, que coincide con lo que piensan el sector de la privacidad[761], es de aplicación la legislación vigente en materia de protección de datos, el RGPD y la LOPDGDD, a todos los datos personales con independencia de que sean visibles o invisibles, es decir, se incluirían los metadatos de carácter personal. Se tratan

[759]Elvery, S. (3 de diciembre de 2018). Mis dispositivos envían y reciben datos cada dos segundos, a veces incluso cuando duermo. *ABC NET AU.* Recuperado de https://www.abc.net.au/news/2018-11-16/datalife-i-spied-on-my-phone-and-here-is-what-i-found/10496450?pfmredir=sm

[760] La mayoría se pueden tratar de actualizaciones de aplicaciones móviles. También investigó si había solicitudes por la noche, y en efecto que las hubo, Apple fue la empresa que más las realizó. El investigador ha declarado que "es extremadamente difícil saber qué solicitudes son útiles para mí y cuáles son simplemente para hacer un seguimiento de mi comportamiento, intereses y hábitos para obtener un beneficio comercial y no me ofrecen ningún beneficio".

[761] Romero, P. (28 enero de 2019). ¿Quién nos protege de nuestros metadatos?. *Público*. Recuperado de https://www.publico.es/sociedad/proteccion-datos-metadatos.html

de datos invisibles que pueden ser utilizados para fines publicitarios o de marketing de salud. En concreto con el Reglamento europeo en la mano habría que tener presente:

i. El principio de minimización de datos. Tanto "Tor" como "Ricochet"[762] podrían posibilitar, a pesar de su dificultad técnica, reducir la cantidad de metadatos. No es cuestión nada baladí puesto que son necesarios para el funcionamiento de las comunicaciones electrónicas.
ii. El principio de limitación de la finalidad (en el sentido de que los metadatos no podrán ser tratados con finalidades incompatibles respecto a las previstas en la información inicial).
iii. El principio de consentimiento (coincide con la obligación de la propuesta del Reglamento de privacidad y comunicaciones electrónicas, pp.18).

Si bien la inclusión de metadatos es necesaria, para facilitar y potenciar un buen número de tareas importantes, también existen problemas asociados y no solamente técnicos como los relacionados con la privacidad[763].

5. LOS HISTORIALES MÉDICOS ELECTRÓNICOS

Con la Directiva 2011/24[764], ya se ofrecía a los Estados miembros la posibilidad de *intercambiar datos sanitarios* pero debido a la heterogeneidad de legislaciones respecto al *acceso de los historiales clínicos electrónicos (HCE)*. La Comisión, en febrero de 2019, hizo públicas unas *recomendaciones*[765] que facilitarían un acceso transfronterizo seguro conforme al Reglamento general de protección de datos." [766].

Por lo que progresivamente se han ido dando introduciendo servicios transfronterizos en todos los Estados miembros de la UE como:

[762] Vid. https://github.com/ricochet-im/ricochet

[763] Otra cuestión que me llama la atención (reflexionando desde el desconocimiento de la ingeniería técnica informática) es el hecho de que estos metadatos y su información estén en texto "orientado a humanos"[763] lo que puede permitir mayor fluidez, comprensión y alcance que si la información no fuera "entendible o legible" para los humanos (y más bien para las máquinas) al margen de los diferentes formatos que estos puedan tener. En todo caso, no debemos perder de vista el impacto de la metadata en los derechos fundamentales y libertades de las personas en general, y en el ámbito del sector sanitario y la Industria del cuidado de la salud, en particular.

[764] Directiva 2011/24 / UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, sobre la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza. Recuperado de https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32011L0024

[765]BOE. Recomendación (UE) 2019/243 de la Comisión, de 6 de febrero de 2019, sobre un formato de intercambio de historiales médicos electrónicos de ámbito europeo.Recuperado de https://www.boe.es/buscar/doc.php?id=DOUE-L-2019-80241

[766]Comisión Europea (21 enero de 2019) Primeros ciudadanos de la UE que utilizan recetas electrónicas de la UE. Recuperado de http://europa.eu/rapid/press-release_IP-18-6808_en.htm

i. La *ePrescripción* y la *eDispensación electrónica* permiten a cualquier ciudadano de la UE recuperar sus medicamentos en una farmacia ubicada en otro Estado miembro de la UE, gracias a la transferencia electrónica de su receta de su país de residencia al país de viaje, posteriormente informando al país de residencia sobre el medicamento recuperado en el país visitado. La *red de eHealth* (el cuerpo de las autoridades de *eHealth* en la UE)[767], por ejemplo, ha dado luz verde desde enero de 2019, a Finlandia y Estonia para comenzar a intercambiar *recetas electrónicas*.

ii. *Los resúmenes para pacientes* brindan información (como alergias, medicamentos actuales, enfermedades previas, cirugías, etc.,) para que en caso de visitas médicas de emergencia en otros países pueda acceder a los mismos. La *red de eHealth* también ha dado luz verde recientemente, por ejemplo, a Czechia y Luxemburgo para recibir resúmenes *de* pacientes de ciudadanos extranjeros[768].

Según la Recomendación (UE) 2019/243 de la Comisión como base de referencia, para un formato de intercambio de historiales médicos electrónicos de ámbito europeo "los Estados miembros deberían adoptar medidas para garantizar que los siguientes dominios de información sanitaria, como base de referencia, formen parte de un formato de intercambio de historiales médicos electrónicos de ámbito europeo: a) historial resumido del paciente; b) receta electrónica/dispensación electrónica; c) resultados de laboratorio; d) imágenes e informes médicos; e) informes de altas hospitalarias.

El intercambio transfronterizo de información debería llevarse a cabo conforme a las normas de referencia, las especificaciones de interoperabilidad y los perfiles en función del dominio de información sanitaria como se establece en el anexo":

Dominios de información sanitaria	Información clínica para el intercambio transfronterizo	Representación de contenidos para el intercambio transfronterizo
Historial resumido del paciente	Estructurado según lo dispuesto en el documento GUIDELINE on the electronic exchange of health data under Cross-Border Directive 2011/24/EU Release 2 – Patient Summary for unscheduled care, adoptado por la red de sanidad electrónica el 21 de noviembre de 2016 (5).	Health Level Seven (HL7) «Clinical Document Architecture (CDA) Release 2» (6) Nivel 3 y nivel 1 (PDF (7)/A)
Receta electrónica/dispensación electrónica	Estructuradas según lo dispuesto en el documento GUIDELINE on the electronic exchange of health data under Cross-Border Directive 2011/24/EU Release 2 – ePrescriptions and eDispensations, adoptado por la red de sanidad electrónica el 21 de noviembre de 2016 (8).	Health Level Seven (HL7) «Clinical Document Architecture (CDA) Release 2» Nivel 3 y nivel 1 (PDF (7)/A)

[767] Comisión Europea. eSalud: salud y atención digital. Recuperado de https://ec.europa.eu/health/ehealth/policy/network_en

[768] En concreto, según el *comunicado de la Comisión Europea de febrero de 2019*, "veintidós Estados miembros forman parte de la *infraestructura de servicios digitales de eSalud* y se espera que intercambien *recetas electrónicas* y *resúmenes de pacientes* para finales de 2021. Diez Estados miembros (Finlandia, Estonia, República Checa, Luxemburgo, Portugal, Croacia, Malta, Chipre, Grecia y Bélgica) pueden comenzar estos intercambios a finales de 2019". Mas info en: http://europa.eu/rapid/press-release_IP-18-6808_en.htm

Imagen 68. Cuadro A: Estructuración y representación de contenidos en los dominios de información sanitaria en relación con los cuales ha adoptado orientaciones la red de sanidad electrónica. Fuente: BOE[769] (Anexo)

A modo de resumen y desde mi opinión convendría recalcar algunos de los principios más importantes que se incluyen en la reciente Recomendación (Anexo):

i. *Sistemas centrados en los ciudadanos desde su diseño y* por defecto para cumplir los requisitos del Reglamento general de protección de datos;

ii. *Protección de datos y confidencialidad.* Los ciudadanos deberían poder ejercer su derecho de acceso a sus datos sanitarios mediante el acceso a sus historiales médicos electrónicos, también a través de las fronteras. En la recomendación se recalca el derecho de protección de datos como "derecho fundamental".

iii. *Consentimiento explícito y otras bases jurídicas* de conformidad con los artículos 6 y 9 del Reglamento general de protección de datos.

iv. *Auditabilidad. "*Los tratamientos de los datos sanitarios deberán archivarse y verificarse a efectos de auditoría, utilizando técnicas apropiadas, como los registros y las pistas de auditoría, para mantener un registro exacto del acceso a los historiales electrónicos, su intercambio o cualquier otra operación de tratamiento".

v. *Seguridad, identificación y autenticación.* Deben asegurarse las medidas técnicas y organizativas para cumplir Reglamento general de protección de datos y de la Directiva (UE) 2016/1148 (SRI respecto a la seguridad. Por *su parte,* el Reglamento (eIDAS) regulará cómo garantizar la confianza en los intercambios de datos (también entre sistemas de historiales médicos electrónicos) a través la identificación y autenticación sólidas y fiables de todas las partes implicadas. De las tres normativas hablaremos más adelante.

6. SALUD, TECNOLOGÍA Y EL DERECHO DE PROTECCIÓN DE DATOS

Ahora bien, dicho esto, ¿qué ocurre con el *derecho de protección de datos en el ámbito de la salud*? Como ya señaló la Comisión hace un par de años; "los *principios de protección de datos* son *esenciales* para lograr los objetivos; permitir el acceso seguro a los datos de salud en toda la UE, compartir datos para una mejor investigación y atención médica personalizada y capacitar a los pacientes con herramientas digitales".

[769] BOE, Recomendación (UE) 2019/243 de la Comisión, de 6 de febrero de 2019, sobre un formato de intercambio de historiales médicos electrónicos de ámbito europeo.Recuperado de https://www.boe.es/buscar/doc.php?id=DOUE-L-2019-80241 .

Pero desde mi opinión no sólo sería importante y necesaria la mera aplicación del marco jurídico de protección de datos sino también, sino también, tal y como estableció el Consejo, "*la seguridad de la información en la red*[770] y *la seguridad de la identificación electrónica*[771] (Consejo de la UE, pto. 24, 2017).

No obstante, al margen de las legislaciones nacionales y de *los principios del tratamiento de datos relativos a la salud*, como señala el Consejo "se necesitarían sistemas y herramientas flexibles que permitan a los ciudadanos *acceder* a sus propios datos, y a la *información* sobre el uso de sus datos, así como gestionar su *consentimiento* para el tratamiento y la comunicación de sus datos sanitarios, incluidos los destinados a un uso secundario" (Consejo de la UE, pto. 15, 2017)[772].

El derecho de los ciudadanos a *tener acceso a sus propios datos sanitarios* es uno de los principios básicos del acervo de la Unión en materia de protección de datos y así se refleja en el Reglamento general de protección de datos. Aunque tal y como establece la Recomendación (UE) 2019/243[773], "la mayoría de los ciudadanos, sin embargo, aún no pueden acceder a sus datos sanitarios (ni compartirlos de forma segura) a través de las fronteras".

El *Comité de Ministros del Consejo de Europa*[774] en una recomendación[775] , el 27 de marzo de 2019, aplicable tanto al sector público como al privado, pide a los gobiernos que transmitan estas directrices a los sistemas de salud y a los actores que

[770] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DO L 194 de 19.7.2016, p. 1) (Directiva SRI).

[771] Reglamento (UE) n.o 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (DO L 257 de 28.8.2014, p. 73) (Reglamento eIDAS).

[772]DOUE (2017). Información procedente de las Instituciones, Órganos y Organismos de la UE. Conclusiones del Consejo sobre la salud en la sociedad digital: avanzar en la innovación basada en los datos en el ámbito de la salud (2017, C-440/05) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017XG1221(01)&from=ES

[773] BOE. Recomendación (UE) 2019/243 de la Comisión, de 6 de febrero de 2019, sobre un formato de intercambio de historiales médicos electrónicos de ámbito europeo. Recuperado de https://www.boe.es/buscar/doc.php?id=DOUE-L-2019-80241. Punto 1.

[774]´Consejo de Europa (28 de marzo de 2019). Protection of health-related data: new guidelines. Recuperado de https://www.coe.int/en/web/human-rights-rule-of-law/home/-/asset_publisher/1qETLXmIMIRe/content/protection-of-health-related-data-new-guidelines?_101_INSTANCE_1qETLXmIMIRe_viewMode=view

[775] Consejo de Europa. Comité de Ministros (27 de m arzo de 2019). Recomendación CM/ Rec (2019) 2 del Comité de Ministros de los Estados Miembros sobre la protección de datos relacionados con la salud. Recueprado de https://search.coe.int/cm/pages/result_details.aspx?objectid=090000168093b26e

procesan datos relacionados con la salud, en particular los profesionales de la salud. y oficiales de protección de datos.

Pero poniendo el punto de mira ya en el Reglamento general de protección de datos, evidenciamos el refuerzo de uno de los principios básicos para el tratamiento de datos personales, como es el consentimiento, eliminando el *consentimiento tácito y* exigiendo que este sea *libre, informado, específico e inequívoco***.** Esto significará que se requiere de una declaración de los interesados o una acción positiva, no pudiendo deducirse en ningún caso del silencio o de la inacción. Además, el consentimiento debe ser *verificable*, y por tanto, esto se traduce en algo realmente relevante por cuanto nos interesa: el responsable o encargado de tratamiento deberá ser capaz de demostrar que el interesado consintió el tratamiento de sus datos personales. Pero además, en el caso de los datos de salud hay una importante novedad, y es que se prohíbe de forma genérica su tratamiento, salvo cuando exista el consentimiento *explícito***.**

Respecto la seguridad citada, el Reglamento señala que los sistemas (de *eHealth*, incluidos) deben estar protegidos, asegurados, ser fiables e integrar la protección de datos *desde el diseño y por defecto*. A este respecto, la nueva Ley Orgánica de Protección de datos y Garantía de Derechos Digitales (LOPDGDD) añade que estos tratamientos de datos de salud *"deberán estar amparados en una ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad"*, y que *"podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte"*.

Sobre el RGPD y la LOPDGDD hablaremos con más profundidad más adelante.

Me gustaría resaltar cuestiones particulares a modo de ejemplo de gran interés a tener en cuenta en el ámbito general de la *eHealth:*

i. Respecto al *deber-derecho de información* del tratamiento de los datos personales de salud (o principio de transparencia), el responsable del tratamiento debe informar al e-paciente de una manera concisa, inteligible y con lenguaje claro y sencillo. Para ello, será recomendable presentar la *información por capas*, como establece la AEPD[776]: "una primera que incluya un

[776] AEPD. Guía para el cumplimiento del deber de informar. Recuperado de https://www.aepd.es/media/guias/guia-modelo-clausula-informativa.pdf

nivel básico de la información requerida, de forma estructurada y muy concentrada, para remitir posteriormente a otra capa que contenga esa información más detallada".

ii. Respecto a la *legitimación jurídica del tratamiento* de datos personales de salud en *eHealth,* no se consideraría obligatorio con carácter general *recabar por escrito el consentimiento* de los e-pacientes para el tratamiento de sus datos personales cuando vayan a ser tele-atendidos en centros sanitarios puesto que se trataría de un "*diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario"*. Pensemos en un escenario donde puedan tratar datos personales para varios fines; uno de asistencia o diagnóstico médico (telemedicina) y otro para fines de investigación dentro de un entorno de sistema DLT o *blockchain* sanitario, por ejemplo. En estos casos la base legitimadora es diferente para cada uno de ellos; en el primero, no requiere de consentimiento, pero en el segundo, sí.

7. MENORES DE EDAD, SALUD, TECNOLOGÍA Y PROTECCIÓN DE DATOS

Al igual que los pacientes de enfermedades graves o crónicas, los menores son grupos sociales vulnerables respecto al derecho fundamental de protección de datos. En la actual Sociedad de la Información, no es raro que cada vez más menores de edad usen aplicaciones móviles de salud como las bucodentales como *"Bad Teeth Doctor"* o como "*Clue"* de control calendario menstrual o las apps de los dispositivos *"Fitbit"* para el ejercicio físico. El legislador ya preveía la necesidad de una mayor protección a los menores.

Antes de nada, conviene entender a qué se refiere el legislador europeo cuando habla de "niños"; *¿se refiere a menores de edad? ¿a menores de edad de una determinada edad? ¿nos encontramos ante una nueva traducción poco precisa y correcta?* Si mantenemos la definición de la *Convención sobre los Derechos del Niño* "todo ser humano menor de dieciocho años de edad, salvo que, en virtud de la ley que le sea aplicable, haya alcanzado antes la mayoría de edad". Por su parte, el artículo 5.1 LOPJM señala que "los menores tienen derecho a buscar, recibir y utilizar la información adecuada a su desarrollo". Tanto el beneficio de los hijos como el desarrollo de la personalidad se consideran por la doctrina límites generales que constriñen las facultades que integran la patria potestad.

Volviendo al derecho de protección de datos, tendremos que tener en cuenta lo establecido por el legislador comunitario y nacional y que afectará de alguna manera al menor dentro del contexto *eHealth,* como por ejemplo:

i. *El lenguaje claro y sencillo*. "Los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender" (considerando 58 RGPD).

ii. *La edad de los menores para otorgar el consentimiento*. Cuando el niño otorgue consentimiento para el tratamiento de sus datos (para uno o varios fines), "en relación con la *oferta directa a niños de servicios de la sociedad de la información*, el tratamiento de los datos personales de un niño se considerará *lícito* cuando tenga *como mínimo 16 años*. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o *autorizó* el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó" (art. 8 RGPD). Quien se tendrá que asegurarse de que las *autorizaciones* sean validas, será el responsable del tratamiento y la autorización debe estar recogida de forma escrita y rellenada en el momento en el que se van gestionar sus datos personales[777].

   El RGPD permitía que los estados miembros puedan establecer por ley una edad inferior a tales fines, siempre que *no sea inferior a los 13 años***.** Un estado miembro podrá decidir si en vez de fijarse la ley con 16 años son 15, son 14 o son 13 pero nunca inferior a los 13. Nuestro legislador la fijó edad en 14 años con la LOPDGDD (art. 7.1)[778].

iii. *Verificación del consentimiento válido y edad del menor.* "El responsable del tratamiento hará esfuerzos razonables para verificar que en tales casos, el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela del niño teniendo en cuenta la tecnología disponible" (Art. 8.2). En la actualidad no todas las verificaciones son las más adecuadas.

   Unos de las mayores discusiones en el momento de la interpretación del RGPD por el sector de privacidad fueron motivados por la búsqueda de mecanismos e instrumentos que garantizaran la licitud del tratamiento y verificación del consentimiento. Los responsables del tratamiento podrían solicitar el *dni electrónico de menores con certificado de autenticación*[779] *(*Rodríguez, Ex director AEPD, 2012) para verificar la edad. La tendencia de futuro, no obstante, será la de la identidad soberana digital (ver Reglamento IDAS) y la implantación del protocolo DLT/*blockchain* en salud en el caso, por ejemplo, de asistencia sanitaria e investigaciones por agencias públicas o laboratorios clínicos privados.

iv. *La edad de los menores para ejercer derechos"(...)los titulares de la patria potestad* podrán ejercitar en nombre y representación de los menores de catorce años los derechos de acceso,

---

[777] La empresa TikTok (musical.ly), la cuarta aplicación más descargada en EEUU, ha sido sancionada en febrero de 2019, con 5 millones de euros por la FTC por haber almacenado los datos de menores de 13 años sin consentimiento de los padres. Recuperado de https://www.washingtonpost.com/technology/2019/02/27/us-government-fined-app-now-known-tiktok-million-illegally-collecting-childrens-data/?utm_term=.502fca43e2f9. Para ver acuerdo disponible en: https://www.ftc.gov/system/files/documents/cases/musical.ly_complaint_ecf_2-27-19.pdf

[778] "El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años. Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

[779] Castelló, C. (11 de diciembre de 2013). El DNI de jóvenes cambia para evitar que mientan con su edad en internet. *CincoDías.* Recuperado de https://cincodias.elpais.com/cincodias/2013/12/10/empresas/1386690018_072015.html

rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente ley orgánica" (Art. 12.6 LOPDGDD)

v. *La autorregulación y códigos de conducta*. "Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o modificar o ampliar dichos códigos con objeto de especificar la aplicación del presente Reglamento, como en lo que respecta a*: la información* proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño" (art. 40.2.g RGPD).

CAPÍTULO VIII. EL NUEVO RÉGIMEN JURÍDICO EN MATERIA DE PROTECCIÓN DE DATOS APLICADO A LA INDUSTRIA DEL CUIDADO DE SALUD DIGITAL

SUMARIO: 1.EL NUEVO MARCO NORMATIVO EUROPEO DE PROTECCIÓN DE DATOS.- 1.1.Antecedentes y proceso de reforma normativa europea. 1.2.El Reglamento (UE) 2016/679 (RGPD). 2.EL NUEVO MARCO NORMATIVO ESPAÑOL DE PROTECCIÓN DE DATOS.- 2.1.Antecedentes de la LOPDGDD. 2.2. La LOPDGDD. 3. LA NORMATIVA SECTORIAL ESPECÍFICA. 3.1.La Ley 14/1986, de 25 de abril, General de Sanidad. 3.2. El Reglamento eIDAS y la Directiva SRI. 4. EL RÉGIMEN JURÍDICO TRATAMIENTO DE DATOS EN LA INVESTIGACIÓN BIOMÉDICA Y ENSAYOS CLÍNICOS.- 4.1.La investigación biomédica. 4.2. Investigación clínica no biomédica. 4.3. Ensayos clínicos. 5. PARTICULARIDADES JURÍDICAS PARA PROYECTOS DE BIG DATA E INVESTIGACIÓN BIOMÉDICA. 5.1. Origen de los datos. 5.2.Finalidades. 5.3.Derechos de los interesados. 5.4.Legitimación . 5.5.Decisiones individuales automatizadas . 5.6.Principios del RGPD aplicables. El papel de los desarrolladores. 5.7.Evaluaciones de impacto. 5.8.Medidas necesarias. 5.9.Buenas prácticas. 5.10.Retos y desafíos. 5.11.Una aproximación a las posibles soluciones 6. PARTICULARIDADES JURIDICAS DE LAS ASEGURADORAS DE SALUD Y PROTECCIÓN DE DATOS A TENER EN CUENTA. 6.1. Finalidades del tratamiento de las aseguradoras. 6.2. Legitimación . 6.3. Cesión de datos personales con finalidad de "selección de riesgos". 6.4. Recogida de datos personales de salud. 6.5.Datos genéticos y aseguradoras.

"Para ser libres es necesario ser esclavos de la Ley"

Marco Tulio Cicerón (43 a.C.)

1. EL NUEVO MARCO NORMATIVO EUROPEO DE PROTECCIÓN DE DATOS

1.1. Antecedentes y proceso de reforma normativa europea

La codificación del derecho a la protección de datos en Europa tiene su origen, en el contexto internacional principalmente, en concreto, en los instrumentos siguientes desarrollados por el Consejo de Europa:

i. En el 1950, por el *Convenio de Derechos Humanos (CEDH).* Este convenio incluye el artículo 8, que garantiza el derecho al respeto de la vida privada y familiar, el domicilio y la correspondencia, además, establece los requisitos para justificar posibles injerencias por parte de las autoridades públicas en el ejercicio de este derecho por parte de las personas.

ii. En 1981, por el *Convenio Europeo del Consejo de Europa para la protección de datos con respecto al tratamiento automatizado de datos de carácter personal* (Convenio 108). Este Convenio se convirtió en el primer instrumento jurídico vinculado y tenía la finalidad de proteger los derechos y libertades de las personas, en el marco del art. 8 CEDH, respecto a los tratamientos automatizados que establecía "no podrán tratarse automatizadamente a menos que el derecho interno prevea garantías adecuadas". [780]

Sus principios fueron alineándose con las Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales por la Organización para la Cooperación y el Desarrollo Económico (OECD). En este contexto, los Estados miembros basándose en los instrumentos internacionales anteriores, iban desarrollando sus propios instrumentos legislativos para abordar el derecho de protección de datos. Así por ejemplo, Alemania, en 1970 codificó por primera vez a nivel internacional una norma de protección de datos *(Datenchutzgesetz Gesetz vom:7.10.1970).* Esto provocó inevitablemente que se creara una suerte de diversidad normativa con diferentes niveles de protección que ponían en peligro al sentido propio del mercado interior de la UE y a la libre circulación de datos. Los esfuerzos nacionales por alcanzar una sintonía armonizadora empezaron a confluir con el objeto de crear y adoptar un instrumento jurídico propio de la UE en materia de protección de datos. Así nació la Directiva 95/46/CE[781][782] relativa

[780] En todo caso tal y como señala la AEPD (PS/00368/2015 R/02202/2015), "las operaciones y procedimientos técnicos automatizados o no, que permitan el acceso –la comunicación o consulta- de datos personales, es un tratamiento sometido a las exigencias de la LOPD (ahora, LOPDGDD)."

[781] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Recuperado de https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML

[782] Vid. Fernández Conte y León Burgos (2016). Antecedentes y proceso de reforma sobre protección de datos en la Unión Europea. En *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad.* Pág. 38. Dtor. Piñar Mañas. Madrid: Editorial Reus. (Como señalan los autores, los objetivos de la Directiva son: "(i) armonizar los instrumentos nacionales de protección de datos mediante la aproximación de legislaciones para asegurar el funcionamiento del mercado interior; (ii) eliminar los obstáculos a la libre circulación de datos personales; (iii) mantener un nivel de protección de

a la protección de datos de las personas físicas en lo que respectaba al tratamiento de datos y la libre circulación de datos personales.

iii. Por su parte, años después, ya en el 2003 con el pleno florecimiento de la era de Internet, el TJUE consideró que la armonización de las legislaciones legales no se trataría de una armonización mínima, sino que supondría una *armonización completa* que asegurara la libre circulación de datos y que garantizara al mismo tiempo un alto nivelo de protección de los derechos e intereses de las personas[783]. Ese mismo año, el TJUE declaraba que la protección de datos no se podía concebir como un *derecho absoluto* en el marco del derecho de la UE, debiéndose considerarse en relación con su función en la sociedad[784]. El nuevo contexto tecnológico y sus posibles consecuencias en materia de protección de datos y seguridad se refleja en el primer informe de la Comisión Europea en 2003, 8 años después. Además, establece un programa de trabajo para que los Estados miembros mejorarán su aplicación donde se especificaba la necesidad de que incrementar su implementación y *sensibilización de derechos y* obligaciones (de titulares y responsables respectivamente), de *modificar legislaciones internas* conforme a la Directiva y asignar recursos suficientes para las autoridades de control, y de reducir las *cargas administrativas.*

iv. En 2007, la *Comisión Europea*, presentó otro informe donde consideraba que no era necesario presentar ninguna propuesta legislativa para modificar la Directiva ya que cumplía con los objetivos originarios y constituía garantía suficiente de alto nivel de protección de datos. En ella se reconoce que hay mejoría en la aplicación por parte de los Estados pero aún siguen algunos que no lo aplican de manera correcta, sin que plantearan problemas reales al mercado interior.

v. En 2009, entró en vigor el *Tratado de Lisboa*[785] marcando un antes y un después en el panorama europeo normativo, concretamente.[786]

vi. Sólo tres años después, en 2010, la Comisión Europea, alarma de algo significativo: se cumplían los objetivos originarios pero *no se adaptaban a la rápida evolución tecnológica y a la*

---

los derechos y libertades de las personas que fuera equivalente en todos los Estados miembros". Esta *Directiva* entró en vigor en 24 de octubre de 1995 y su plazo de trasposición finalizó el 24 de octubre de 1998. Dicha trasposición no se realizó de la forma prevista lo que derivaría que la Comisión Europea iniciara procedimientos de infracción contra varios Estados miembros).

[783] Tribunal de Justicia de la Unión Europea, caso *Bodil Lindqvist,* demanda núm. C-101/01, Sentencia de 6 de noviembre de 2003, p.29. Accesible en : https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62001CJ0101&from=EN

[784] Tribunal de Justicia de la Unión Europea, caso *Eugen Schmidberger, Internationale Transporte und Planzüge contra Republic Österreichm ¡,* demanda núm. C-112/00, Sentencia de 6 de noviembre de 2003, p. 80. Accesible en : http://curia.europa.eu/juris/liste.jsf?language=en&num=C-112/00

[785] Tratado de Lisboa por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea, Diario Oficial de la Unión Europea, C 306/1 DE 17 DE DICIEMBRE DE 2007. Accesible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A12007L%2FTXT

[786] Vid. Fernández Conte y León Burgos (2016). Pp. 40-41. (Como señalan los autores, "dió lugar a dos cambios constitucionales significativos en la estructura del derecho de la Unión Europea en materia de protección de datos: (i) la *Carta de Derechos Fundamentales de la Unión Europea* pasó a ser jurídicamente vinculante y, con ello, se elevó el derecho a la protección de los datos personales a la categoría de derecho fundamental independiente, en particular, mediante la inclusión de manera expresa de la protección de datos de carácter personal entre las libertades fundamentales (Art. 8); (ii) la introducción de una disposición específica en el *Tratado de Funcionamiento de la Unión Europea* que codifica el derecho de toda persona a la protección de los datos de carácter personal (art. 16 TFUE)").

globalización[787]. Para proceder a la formulación de la propuesta legislativa la CE se embarcó en un amplio proceso de *consulta*[788] con todas las partes involucradas, donde se confirmó la necesidad de modernizar el marco jurídico de la protección de datos personales en la Unión Europea" (Fernández Conte y León Burgos, 2016, 40).

vii. Finalmente, este proceso se acabaría materializando en la propuesta legislativa del RGPD, dos años después, en 2012. Estos autores destacan la importancia de los indicadores del *Eurobarómetro*[789] publicado en 2011 respecto a las actitudes relacionadas con la protección de datos y su preocupación por cómo las empresas usaban sus datos y sentían la necesidad de tener derecho a borrar su información personal disponible en línea. También se deducía del mismo el apoyo consolidado social para una armonización de la normativa más fuerte. En definitiva, la convergencia el nuevo Tratado de Lisboa, el contexto de la evolución de las tecnologías, la implicación de la opinión pública, o mejor dicho, la importancia de los resultados de la consulta pública derivaron en el eminente proceso de reforma por parte de las instituciones comunitarias. Ocurriría algo determinante e importante: se trataría de un proceso de reforma no basado en "los intereses de los *lobbies*, sino partiendo de opiniones expertas y, principalmente, de una necesidad social previamente constatada que constituiría, a su vez, un factor decisivo a lo largo del proceso legislativo" (Fernández Conte y León Burgos, 2016, 42).

viii. La *Comisión Europea* realizó una *evaluación de impacto*[790] valorando diferentes escenarios de actuación basándose en tres objetivos estratégicos ; mejorar la dimensión del mercado interior, lograr un ejercicio efectivo de los derechos de los ciudadanos y un marco general y coherente que abarque todos los ámbitos de competencia de la Unión. Se pensó que el mejor instrumento jurídico que podría ayudar a cumplir esos objetivos sería el Reglamento gracias a su

---

[787] Para ello, señalaba una serie de retos específicos que requerían nuevas soluciones y enfoques legislativos como; "(i) abordar el impacto de las nuevas tecnologías; (ii) reforzar la dimensión del mercado interior de la protección de datos; (iii) hacer frente a la globalización y mejorar las transferencias internacionales de datos; (iv) consolidar las disposiciones institucionales para la aplicación efectiva de las normas sobre protección de datos; (v) mejorar la coherencia del marco jurídico que regula la protección de datos". En este sentido, "la Comisión Europea planteó los objetivos sobre los que se basaría la futura propuesta legislativa que modificará, a la postre, la Directiva de protección de datos. Estos objetivos fueron; "(i) reforzar los derechos de las personas; (ii) profundizar en la dimensión del mercado interior; (iii) revisar las normas de protección de datos en los ámbitos de la cooperación policial y judicial en materia penal; (iv) tener presente la dimensión global de la protección de datos.

[788] Según Fernández Conte y León Burgos (2016, 41); "obtuvo un total de 288 respuestas de personas y entidades, donde participó la Abogacía Española la cual participó en la formulación de los posicionamientos jurídicos del CBBE (Consejo de la Abogacía Europea) sobre cuestiones sobre el RGPD, al igual que la AEPD con la preparación de recomendaciones y pautas para despachos de abogados en el uso de *cloud computing"*.

[789] Comisión Europea (junio de 2011). Eurobarómetro Especial 359. Attitudes on Data Protection and Electronic Identity in the European Union. Recuperado de http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf

[790] Comisión Europea (25 de enero de 2012). Comission Stadd Working Paper. *Impact Assesment*. Regulation of the European Paliament and of the Council on the protection of individuals with regard to the processing of personal data on the free movement of such data (RGPD) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data . Recuperado de https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0072&from=EN

aplicabilidad directa (art. 288 TFUE[791]), el cual reduciría la fragmentación jurídica otorgando mayor seguridad jurídica.

Además este instrumento jurídico se basaría en el art. 16 TFUE[792]. El proceso de toma de decisiones que se iba a iniciar para arrancar la máquina legislativa se basaría en el procedimiento legislativo ordinario o por "codecisión" entre el Parlamento y el Consejo Europeo.

1.1.1. La propuesta del Reglamento General de Protección de Datos (RGPD).

El 25 de enero de 2012, la Comisión Europea presentó la propuesta[793] del Reglamento al Parlamento y al Consejo relativo a la protección del tratamiento de datos de las personas físicas y a la libre circulación de dichos datos.

i. El papel del Parlamento Europeo.

En primer lugar, hablemos de cómo transcurrió la tramitación parlamentaria. Se asignó en 2012, un comité que fue el Comité de Libertades Civiles, Justicia y Asuntos de Interior (LIBE) cuyo ponente principal fue *Jan Philipp Albrecht* que junto con la

[791] Señala que "para ejercer las competencias de la Unión, las instituciones adoptarán reglamentos, directivas, decisiones, recomendaciones y dictámenes. El reglamento tendrá un alcance general. Será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro. La directiva obligará al Estado miembro destinatario en cuanto al resultado que deba conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y de los medios. La decisión será obligatoria en todos sus elementos. Cuando designe destinatarios, sólo será obligatoria para éstos. Las recomendaciones y los dictámenes no serán vinculantes".

[792] Señala que "1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes. Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea."

[793] Según Fernández Conte y León Burgos (2016, 44) , los objetivos declarados eran: "(i) permitir a los ciudadanos tener una mejor información, acceso y control sobre sus datos personales; (ii) incrementar la seguridad del procesamiento de estos; (iii) mejorar la eficacia de los derechos; (iv) incrementar la confianza de los consumidores en el comercio transfronterizo; (v) el derecho a rectificación y al borrado de datos; (vi) el derecho a denegar el procesamiento; (vii) el establecimiento de una autoridad independiente supervisora; (viii) recursos, responsabilidad y sanciones" . (Ya en la propuesta aparecen los nuevos elementos como el principio de transparencia y la *responsabilidad proactiva* de los responsables de tratamiento de datos, además del derecho al olvido).

Comisaria de Justicia *Viviane Reding* se convirtieron en protagonistas de esta fase del proceso[794].

A mediados de 2012, se convocó una audiencia donde se hablarían de las cuestiones clave relativas al ámbito de aplicación, el consentimiento de titulares, intereses legítimos de los responsables de tratamiento, el derecho al olvido y las sanciones.

Al año siguiente, en enero de 2013[795], se incorporan las siguientes propuestas de reforma a la propuesta de Reglamento: (i) "el Reglamento debería aplicarse a todas las actividades de tratamiento relacionadas servicios independientemente de que estos sean gratuitos; (ii) deben incorporarse definiciones para los términos pseudónimo, transferencia, profiling y productor; (iii) debe reformularse la previsión del uso de datos basados en intereses legítimos de seguridad jurídica; (iv) normas estrictas de protección al consumidor (el consentimiento deja de ser efectivo si el tratamiento no es necesario y la ejecución de un contrato o la prestación de un servicio no puede ser condicionada al consentimiento del tratamiento o uso de datos que no sean necesarios; (v) el criterio es el de residencia europea del titular de los datos; (vi) la autoridad europea de protección de datos debería estar implicada en la adopción de algunos estándares y actos de la Comisión; (vii) el derecho de objeción al tratamiento debe ser gratuito y estar claramente expresado; (viii) mejoras del sistema de sanciones de las autoridades de supervisión; (ix) los datos de menores y otros datos sensibles deben emplearse con su consentimiento"

ii. El papel del Consejo Europeo

[794] Según Fernández Conte y León Burgos (2016, 45); "varios elementos intrínsecos y externos (lobbies) influyeron en el calendario de aprobación que se retrasó casi seis meses entre la fecha inicialmente prevista para el voto de su Comité y su celebración real".

[795] Dos meses después, se presentaron casi 4.000 enmiendas de las que fueron válidas 2.600. El informe definitivo se aprobó en octubre con más de 90 enmiendas. El *Comité LIBE* "aprobó un mandato para abrir negociaciones informales o *"tripartitos"* con el *Consejo* (y con participación de la Comisión) que, sería decisivo para el éxito del procedimiento" (Fernández Conte y León Burgos, 2016, 45). Los sucesos acontecidos en relación al caso *Snowden* (vigilancia masiva y suministro de datos que poseían empresas a Estados) tuvieron bastante repercusión en el momento sensible de la tramitación de este Reglamento, "dado que el texto de negociación del Parlamento Europeo estaba cerrado antes de sus revelaciones". Como consecuencia de esto último, el Parlamento Europeo decidió investigar acerca del impacto que tenía este tipo de hechos sobre los derechos fundamentales de los ciudadanos y publicó una resolución al respecto. Estaba claro que esta cuestión no resultaría indiferente al proceso y afectaría de alguna medida a la tramitación.

A partir de junio de 2015[796], se inician los diálogos *"tripartitos"* que acercarán el proceso al acuerdo final sobre esta nueva normativa. Como dijimos los tripartitos son reuniones informales e interinstitucionales que impulsan y permiten avanzar de alguna manera las negociaciones. En tanto, el SEPD también emitió recomendaciones para alimentar a estos foros. En noviembre de 2015, en el último tripartito se contemplaban cuestiones que preocupaban como eran el tratamiento de datos a efectos de investigación, la forma de expresar el consentimiento, es decir, qué es el consentimiento y cuándo se necesita, y las obligaciones de los responsables y encargados de tratamiento. Finalmente, el 15 de diciembre, las negociaciones del tripartito resultaron en una propuesta conjunta, ratificándose por el Consejo en febrero de 2016, aprobándose en abril de 2016 por el Parlamento (por el comité LIBE primero, y después, por el pleno).

Comisión	**Consejo**	**Parlamento**
• Poder ***ejecutivo*** e iniciativa legislativa • Propone legislación, aplica decisiones y defiende los Tratados. • Actúa a modo de "Consejo de Ministros" y hay un representante por cada Estado miembro (28 comisarios).	• Función ***legislativa.*** • Proc. leg.ord: se requiere tanto del voto del Consejo como el del Parlamento. • Es un órgano de naturaleza intergubernamental, orientación política colectiva: representan la posición del ejecutivo de su E.M.	• Función ***legislativa*** • Sus componentes son elegidos por los ciudadanos de la UE

Tabla 44. Diferencias funcionales básicas entre Instituciones Comunitarias Europeas.

1.1.2. La aprobación del Reglamento General de Protección de Datos (RGPD)

Finalmente, el 27 de abril de 2016, el "Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de datos de las personas

[796]Desde 2012 el Consejo se empezaron a celebrar, una serie de reuniones de expertos de Estados miembros (denominado como "Grupo DAPIX", grupo de trabajo sobre intercambio de la información y protección de datos). El papel del Consejo que es definir las orientaciones y prioridades políticas generales de la UE, aprobó en octubre de 2012 sus conclusiones que apremiaban la adopción del Reglamento. Aunque el Consejo no sea precisamente una institución comunitaria legislativa, "tuvo un papel importante para impulsar el proceso político en algunos de sus momentos más críticos, al igual que el de la vicepresidenta y comisaria de Justicia y el ponente parlamentario *Albrecht*". Las reuniones de 2014 trataban cuestiones del ámbito territorial, varias definiciones, transferencias internacionales, etc. En octubre, "se alcanzó un nuevo enfoque parcial general sobre el capítulo IV acerca de las obligaciones de los responsables y encargados" (Fernández Conte y León Burgos, 2016, 47). Al igual que el caso *Snowden* "sensibiliza" de alguna manera al proceso de reforma con la sentencia *Google* [796] contra España sobre el derecho al olvido que es analizada por los Estados miembros. En marzo de 2015, se llevaría a cabo una de las reuniones más importantes donde se abordaron cuestiones sobre los principios generales especialmente acerca del "consentimiento" y la ventanilla única.

físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE", fue publicado en el Diario Oficial de la Unión Europea"[797]. Debido a que la nueva legislación tendrá una gran repercusión y necesitará ajustarse a aspectos significativos, los Estados miembros y las partes interesadas tendrán que prepararse plenamente para ese nuevo marco jurídico. Es por ello, que se estableció un periodo transitorio de dos años hasta el 25 de mayo de 2018. Del 2016 al 2018, todas las partes interesadas, administraciones nacionales, autoridades nacionales de protección de datos, responsables y encargados de tratamiento han llevado a cabo determinadas actividades a fin de intentar garantizar la importancia y el alcance de los cambios que traía esta nueva normativa.

En este sentido, la Comisión comunicó una serie de orientaciones[798] para realizar la mejor adaptación posible antes que llegara la fecha de su aprobación y organizó una serie de eventos para llegar a las partes interesadas *("stakeholders")* como talleres para consumidores, debates sectoriales de investigación y servicios financieros.

Según la Comisión y respecto a las grandes organizaciones, "algunos operadores recurren a *listas de comprobación del cumplimiento* (tanto interno como externo), solicitan asesoramiento a sociedades de consultoría y bufetes de abogados y buscan productos que se adecuen a los requisitos de protección de datos desde el diseño y por defecto. Cada sector debe elaborar mecanismos que sean adecuados a la naturaleza específica de su ámbito y que se adapten a su modelo de negocio. Las empresas y otras organizaciones que realizan el tratamiento de datos también podrán aprovechar las nuevas herramientas previstas en el Reglamento como elemento para demostrar el cumplimiento, tales como *códigos de conducta y mecanismos de certificación"*. Por otro lado, la Comisión ha creado también un grupo multilateral sobre el Reglamento, compuesto por representantes de la sociedad civil y del sector empresarial,

[797] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679

[798] Comisión Europea (24 enero de 2018). Comunicación de la Comisión al Parlamento Europeo y al Consejo. Mayor protección, nuevas oportunidades: Orientaciones de la Comisión sobre la aplicación directa del Reglamento general de protección de datos a partir del 25 de mayo de 2018. Recuperado de https://ec.europa.eu/transparency/regdoc/rep/1/2018/ES/COM-2018-43-F1-ES-MAIN-PART-1.PDF

representantes del mundo académico y profesionales el cual asesorará a la Comisión[799]. Este grupo "asesorará, en concreto sobre el modo de lograr un *nivel adecuado de sensibilización* sobre el Reglamento en las partes interesadas"[800][801].

Finalmente, en el 25 de mayo de 2018 se aprobó el Reglamento general de protección de datos (Reglamento UE 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos derogando la Directiva 95/46/CE).

Con el Reglamento en vigor, la Comisión ha declarado en una comunicación [802] en noviembre de 2018, que ha ido observando que varias autoridades de protección de datos han informado de un aumento del número de reclamaciones.

En resumen, el papel de liderazgo en materia de privacidad (comunicaciones, vida privada y familiar, y protección de datos) que asume la UE es bastante evidente. Los primeros comienzos normativos vinieron sustentándose dos grandes y originarios instrumentos internacionales: el CEDH y el Convenio 108. Pero la primera regulación llegaría en forma de *Directiva europea* para e*volucionar* a *Reglamento europeo*, dejando de ser objetivo estrechamente relacionado con el mercado común interior para pasar a ser "derecho fundamental" (Fernández y León, 2016, 49).

---

[799] Vid. Grupo de expertos de múltiples partes interesadas para apoyar la aplicación del Reglamento (UE) 2016/679 (E03537). Recuperado de http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537

[800] También "la Comisión Europea, a través de, Iniciativa Horizonte 2020, ha financiado acciones para desarrollar *herramientas* que apoyen la aplicación efectiva de las normas relativa al *consentimiento* y sobre los métodos de protección de la privacidad de los análisis de datos, tales como la informática compartida y el cifrado homomórfico". (Vid. Comisión Europea. Secciones Horizonte 2020. Recuperado de https://ec.europa.eu/programmes/horizon2020/h2020-sections) . Es de destacar la importancia que otorga la Comisión en estas medidas donde se celebra un talle específico para datos sanitarios en octubre de 2017.

[801] Por otra parte, el 23 de mayo de 2018, se publicó en el Diario Oficial de la Unión Europea un listado de correcciones al RGPD en diferentes idiomas que, aunque suponía cambios menores, destaca uno de ellos en concreto por su importancia. Se refiere al ámbito de aplicación del RGPD regulado en su artículo 3.2, por el que se sustituye la palabra "*interesados que residen en la Unión"* por *"interesados que se encuentren en la Unión"*. Se detecta una traducción poco precisa entre las versiones inglesa y española. Vid. DOUE, 23 de mayo 2018. Corrección de errores del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD Recuperado de https://www.boe.es/doue/2018/127/L00003-00007.pdfhttps://www.boe.es/doue/2018/127/L00003-00007.pdf.

[802] Comisión Europea (8 de noviembre de 2018). Answer by Ms. Jourovà on behalf of the European Commission. Recuperado de http://www.europarl.europa.eu/doceo/document/E-8-2018-004999-ASW_EN.pdf

Para comprender el proceso de reforma, se recomienda una reflexión contextual jurídico-social a partir de la cual se pueda detectar la relevancia de los grupos de interés *("stakeholders"*) y los sucesos judiciales que iban produciéndose paralelamente[803].

1.2. El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (RGPD)

1.2.1. El objeto, ámbito de aplicación y definiciones.

Según Piñar Matas (2016,53)[804] "*el objeto es doble*: regular un derecho (protección de datos) y garantizar una libertad (la libre circulación de los datos). En este sentido es muy esclarecedor el considerando 166 "los objetivos del presente Reglamento son proteger los derechos y las libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales, y garantizar la libre circulación de los datos personales en la Unión". El marco de referencia de ambos es ahora el RGPD sin olvidar el alcance económico que tienen los datos en la actualidad (considerando 2) [805].

No obstante, "el derecho fundamental prevalecerá sobre el interés económico de los responsables y encargados como ya señaló el TJUE en su sentencia de 13 de mayo de 2014, *Google Spain* y Agencia Española de Protección de Datos (AEPD), asunto C13/12". Además, por otra parte, el Reglamento es consciente de que la innovación

[803] La participación de los personas interesadas es fundamental, nos referimos a organizaciones o compañías, asociaciones de consumidores y usuarios, ONGs, asociaciones profesionales, consorcios corporativos, ciudadanía,..etc. Pero además, hay que tener en cuenta que el legislador no es experto en tecnología, ni en ingeniería informática o telemática, por lo que para conocer determinadas cuestiones ha tenido que ser necesaria la intervención de expertos conocedores de la materia. Las tecnologías emergentes están produciendo escenarios disruptivos que se irán traduciendo en adaptaciones y ajustes del nivel de protección de datos para minimizar los impactos a los derechos fundamentales de las personas (ciudadanos, consumidores, etc.). El papel de los investigadores y de las universidades, además de sectores de la abogacía y medicina será esencial.

[804] Piñar Mañas, J.L. (2016). Objeto del Reglamento. En *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad.* Págs. 51-62.Madrid: Editorial Reus.

[805] El legislador señalaba que; "Los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea su nacionalidad o residencia, respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos de carácter personal. El presente Reglamento pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas".

tecnológica tiene una incidencia capital en la protección de datos, pero que ha de alcanzarse necesariamente un equilibrio entre una y otra (considerando 6)[806].

Respecto al ámbito de *aplicación territorial* (Art. 3 RGPD), diremos que se distinguen dos supuestos (RIPOL, 2016, 95)[807].

En el primero, el RGPD se aplicará en todos los casos en que el tratamiento se realice en el contexto de las actividades del *establecimiento*, con independencia de dónde se realice el tratamiento y dónde *"se encuentre"* el interesado. El concepto "establecimiento" se extiende a cualquier actividad real y efectiva aún mínima ejercida mediante una instalación estable, por ejemplo, Google España. Así por ejemplo, recientemente el Tribunal Supremo (STS 121/2019, de 5 de febrero, Rec. 627/2018) ha establecido que la Agencia Española de Protección de Datos (AEPD) es competente para sancionar a una sociedad domiciliada en otro país de la Unión Europea pero que opere de forma regular en España[808]. Y es que "sólo de esta forma se supera la rigidez y el formalismo, al no ser equivalente el concepto de establecimiento al de la sede social donde esté registrada la sociedad responsable del tratamiento de datos".

En el segundo, el RGPD especifica que el Derecho de la UE se aplicará a los responsables del tratamiento afecte a residentes de la UE y siempre que *ofrezcan bienes*

---

[806] El legislador sigue señalando que; "La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales".

[807] Ripol Carulla, S. (2016) Aplicación territorial del Reglamento. En *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad.* Págs. 77-95. Dtor. Piñar Mañas. Madrid: Editorial Reus.

[808] Noticias Jurídicas. (18 de marzo de 2019). La AEPD es competente para sancionar a una entidad con sede en Luxemburgo y con apartado de correos y cuenta bancaria en España. Recuperado de *NoticiasJurídicas.* Recuperado de http://noticias.juridicas.com/actualidad/jurisprudencia/13789-la-aepd-es-competente-para-sancionar-a-una-entidad-con-sede-en-luxemburgo-y-con-apartado-de-correos-y-cuenta-bancaria-en-espana/
(Se trataba de "una sociedad domiciliada en Luxemburgo dirigía, de forma regular, actividades y operaciones a través de medios instrumentales radicados en España, pues disponía de un apartado de correos y era titular de una cuenta corriente en España. Este tratamiento de datos se articulaba en virtud de un contrato de compraventa de una cartera de créditos celebrado en España, siendo gestionados los cobros por una entidad domiciliada en España, que se encargaba de las reclamaciones e incidencias en relación con las obligaciones de pago que resultaban incumplidas. La Agencia Española de Protección de Datos impuso una sanción a la entidad luxemburguesa, y posteriormente la Audiencia Nacional estimó que la Agencia carecía de competencia para imponer tal sanción, al estar la empresa sancionada domiciliada en un tercer Estado miembro de la Unión Europea").

y servicios a ciudadanos de la UE, o cuando se proceda a algún control de su comportamiento" Las actividades del tratamiento se refieran a un objeto determinado que puede ser bien, la oferta de bienes o servicios a dichos interesados, por ejemplo, la página web, el idioma o moneda o bien, la observación del comportamiento de dichos interesados en la medida que este comportamiento tenga lugar en la Unión Europea. El sentido de este artículo va acorde al objetivo del Reglamento,-a diferencia de la Directiva que trataba armonizar la protección de las normas estatales de protección de datos-, y es establecer un nivel de protección equivalente en todos los Estados miembros y garantizar una aplicación coherente y homogénea de estas normas.

Es de mencionar que antes de su entrada en vigor, se publicó en el Diario de la Unión Europea un documento en el que recogían correcciones menores donde una de ellas afectaba de lleno a este artículo (art. 3.2): se sustituiría la palabra interesados que "*residen*" en la Unión por interesados que "*se encuentren***"** en la Unión**.**

Por otro lado, el ámbito de *aplicación material*[809] (Uriarte Landa, 2016, 76) parece coincidir con el de la Directiva, "incluye algunos matices, redefine las excepciones, manteniendo la esencia de las mismas, a la vez que actualiza el ámbito material de la Directiva, esencialmente en los considerandos en lo que respecta a las redes sociales".

Respecto a las *definiciones*, es de destacar la ampliación del número de conceptos incluidos (26 términos, exactamente) de los cuales únicamente 8 coinciden con la Directiva (art.2) "introduciéndose adaptaciones a la evolución tecnológica y se aproximan así a la realidad a la que deben de ser aplicados"[810].

---

[809] Uriarte Landa, I. (2016).Ámbito de Aplicación material. En *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad.* Págs. 63-76. Dtor. Piñar Mañas. Madrid: Editorial Reus. (Como señala el autor, el RGPD, a su vez, "expresa la no aplicación a los tratamientos que realicen las autoridades competentes de cada Estado con fines de persecución de infracciones penales, mientras que mantiene su aplicación, para el resto de los tratamientos que puedan realizar con otras finalidades. Refuerza la idea de aplicabilidad de las normas de protección de datos a los prestadores de servicios de la sociedad de la información y en especial a los prestadores de servicios de intermediación". Pero además, recoge e incluye en el ámbito material a los tratamientos de órganos e instituciones comunitarias , igualándolos a las entidades privadas y públicas).

[810] Algunos llaman la atención y serán de gran importancia como las normas vinculantes empresariales *("corporate binding rules")* y otros necesarios que se adaptan al contexto tecno-social de la normativa como "servicio de la sociedad de la información" (aunque no es novedad ya que está incluido en la Directiva (UE) 2015/1535, art.1). En los mismos encontraremos conceptos que pertenecen a disciplinas más técnicas como podría ser la de ingeniería informática o similar, como podrían ser: pseudonimización, anonimización, violación de la seguridad de los datos, datos biométricos, elaboración de perfilados *("profiling"),* dirección IP, correo electrónico, datos disociados, etc.

1.2.2. Principios del derecho a la protección de datos

Según Puyol Montero (2016, 135-6) [811], "los *principios* [812] están formados por un conjunto de reglas que determinan cómo se deben recoger, tratar y ceder los datos de carácter personal, a los efectos de garantizar la intimidad y demás derechos fundamentales de los titulares de los datos, los consumidores o usuarios, y en definitiva, los ciudadanos". Es más, podríamos llegar a afirmar que "los principios generales de protección de datos constituyen el contenido esencial del derecho a la protección de datos, y que, a través de los mismos, se configura un sistema de tutela que garantiza una utilización más racional y razonable de los datos personales". Además, tal y como establece este autor, no sería conveniente considerarlos (únicamente) a éstos como principios de obligaciones del responsable del tratamiento, puesto que tienen un alcance y trascendencia de mayor envergadura. No solamente afectan al responsable del tratamiento, sino a todas aquellas personas físicas o jurídicas que intervienen en el tratamiento de datos, sirviendo como pauta normativa e interpretativa a todas las instituciones jurídicas donde existe un tratamiento de datos de carácter personal.

i. Principios relativos al tratamiento.

Los principios relativos al tratamiento en el RGPD (art.5) tienen un marcado "carácter continuista" (PIÑAR, 2016, 136)[813] con la que ya se contenía en la Directiva y en la antigua LOPD 15/1999. Antes se afirmaba que "sólo estaba permitida la recogida y el tratamiento cuando los mismos eran adecuados, pertinentes y no excesivos en

[811] Puyol Montero, J. Los principios del Derecho a la Protección de datos. En *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad.* Págs. 235-150. Dtor. Piñar Mañas. Madrid: Editorial Reus. Tal y como señala muy acertadamente este autor , además "deberán ser considerados tanto en la elaboración como en la aplicación de las normas, y, por otro lado, también son utilizados para hallar las soluciones concretas a casos y supuestos determinados en defecto de normativa aplicable". Son de gran utilidad para la materia de protección de datos, ya que pueden suplir directamente "las múltiples lagunas legales que pueden producir la propia regulación a consecuencia de la imparable evolución de la tecnología". Por tanto, tal y como establece el profesor, éstos gozan de especial importancia y trascendencia en el nuevo Reglamento, ya que entre otras cosas, "sirven a los operadores jurídicos que intervienen en la materia a los efectos de que puedan cumplir de manera satisfactoria las exigencias jurídicas y de responsabilidad social empresarial vinculadas a las nuevas exigencias y requerimientos derivados de la protección de datos de carácter personal".

[812] Del art. 5 al 11 RGPD, se establecen los principios relativos al tratamiento, la licitud, las condiciones para recabar el consentimiento, los requisitos aplicacables al consentimiento prestado por el niño en relación con los servicios de la Sociedad de la Información, los tratamientos de categorías especiales de datos personales, los tratamientos de datos personales relativos a condenas e infracciones de naturaleza penal, y finalmente, los tratamientos que no requieren una especial identificación.

[813] Cfr. Piñar Mañar, J.L. Jornadas ENATIC sobre "El nuevo Reglamento Comunitario de Protección de Datos" , CGAE, Madrid, 29 de abril de 2016.

relación con el ámbito y las finalidades determinadas, explícitas, y legítimas para las que se habían obtenido los datos, en ese momento dichos valores se matizan, en el sentido de que el tratamiento sea lícito, leal y transparente" (PUYOL, 2016, 136).

Como manifestación de una de los mayores objetivos del RGPD de empoderar al titular de datos a la hora de tomar decisiones acerca del tratamiento de sus datos, la exigencia del *principio de transparencia* en la forma de recabar el consentimiento y de dicho tratamiento juega un papel muy importante. Esto facilitará al titular tomar las decisiones con conocimiento de causa.

Por otro lado, se encuentra el *principio de limitación de tratamiento* que se refiere al hecho de que no se pueden tratar datos personales con un propósito o finalidad diferente que aquella que expresamente ha sido consentida por parte del titular de los datos para posibilitar legalmente dicho tratamiento.

También hemos de señalar el *principio de minimización* que consiste en que en el momento de la recolección de datos, no se puedan solicitar del titular de los mismos más datos que aquellos que estrictamente son necesarios y además dicha solicitud ha de encontrarse justificada en función de la naturaleza y finalidad del tratamiento. De igual manera, se pide que los datos sean exactos, y actualizados, exigiendo al responsable medidas suficientes en el caso de su supresión o rectificación. Pero además, "la vinculación entre el titular de los datos y los datos que se contengan en la base de datos tiene que ser el estrictamente necesario en función del tratamiento para el cual se ha recabando el consentimiento del interesado" (PUYOL, 2016, 139). Fuera del cumplimiento de esta finalidad, los datos solo se podrán conservar de manera asociada con relación a archivos de interés públicos, tales como de investigación científica, etc. Es lo que se denominaría como *principio de limitación del plazo de conservación.*

Los datos, además, tienen que ser tratados de forma que garantice una seguridad adecuada, y la protección contra el tratamiento no autorizado o ilícito, y contra posibles pérdidas, destrucciones o daños accidentales por medio de medidas organizativas y técnicas. Y esto se denominaría *principio de integridad y confidencialidad de los datos.*

Por último, no podemos olvidar el tan mencionado *principio de responsabilidad proactiva,* que implica que el responsable del tratamiento tiene que garantizar la licitud, la lealtad y la transparencia en todo el proceso del tratamiento de datos con relación al

interesado. Pero no sólo esto, el legislador obliga al responsable que acredite que efectivamente el tratamiento cumple lo establecido en el art. 5.1. RGPD.

ii. Licitud del tratamiento.

El art. 4.7 de la antigua LOPD ya prohibía expresamente la recogida de datos por medios fraudulentos, desleales o ilícitos. *El Reglamento europeo establece en el art. 5.1:*"Los datos personales deben ser tratados de *manera lícita,* leal y transparente en relación con el interesado". Concretamente en el art. 6 del Reglamento europeo establece lo siguiente en relación con la licitud del tratamiento: "El tratamiento solo será lícito si se cumple *al menos una* de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para *uno o varios fines específicos*;
b) el tratamiento es necesario para la ejecución de un *contrato* en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
c) el tratamiento es necesario para el cumplimiento de una *obligación legal* aplicable al responsable del tratamiento;
d) el tratamiento es necesario para proteger *intereses vitales* del interesado o de otra persona física;
e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el *ejercicio de poderes públicos* conferidos al responsable del tratamiento;
f) El tratamiento es necesario para la satisfacción de *intereses legítimos* perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño".

Por otro lado, en el apartado segundo, se habilita a los Estados miembros a que puedan mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento, con relación a la licitud del tratamiento.

1.2.3. Responsabilidad activa

El Reglamento presenta un nuevo modelo donde cabe la mejora continua para plantea garantizar los derechos y libertades de las personas, evitando la posibilidad de daños y perjuicios para los interesados que puedan llegar a materializarse. Se trata, en

definitiva de un modelo proactivo que lleva asociada la obligación de responsables y encargados del tratamiento de estar en disposición de "demostrar" en todo momento actúan con cierta diligencia. El legislador comunitario se refería a este principio como a la *"accountability",* un concepto que no tiene traducción al castellano y que es heredado de la cultura anglosajona empresarial. La intención del legislador no es otra que la de que los propios responsables y encargados de los tratamientos asuman la responsabilidad de decidir el marco de desarrollo de los mismos, tomando decisiones que en todo momento permitan establecer garantías para los derechos y libertades de las personas. El objetivo último no es fijar unas normas estáticas de cumplimiento sino más bien de asignar la obligación de decidir sobre qué medidas hay que optar que consigan esas garantías.

Pero, ¿de qué obligaciones se habla?

1.2.3.1. Elaboración de un registro de actividades de tratamiento (Art. 30)

En él se detallarán los tratamientos que el responsable llevará a cabo y contendrá cuestiones como: Nombre y datos de contacto del responsable o corresponsable y del DPO si existiese, finalidades del tratamiento, descripción de categorías de interesados y categorías de datos personales tratados y transferencias internacionales de datos. Estarán exentas las organizaciones que empleen a menos de 250 trabajadores, a menos que el tratamiento que realicen pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional o incluya categorías especiales de datos o datos relativos a condenas e infracciones penales. El registro constará por escrito, incluido en formato electrónico. A continuación, se señala un cuadro con el contenido de dicho registro tanto para el responsable como para el encargado.

	Responsable	**Encargado**
Datos identificativos y de contacto	Responsables Corresponsables Representante del responsable DPO	Encargado Otros encargados Representante del encargado Responsables Representantes de responsables DPO
Descripción del tratamiento	Finalidades del tratamiento Descripción de las categorías personas e interesados Descripción de las categorías de datos	Descripción de las categorías de datos personales Descripción general de medidas técnicas, organizativas y de seguridad

	personales Descripción general de medidas técnicas, organizativas y de seguridad Plazos de supresión	
Transferencias internacionales	Descripción de las transferencias Identificación de los países de destino Identificación de organización internacional La documentación que aporte garantías adecuadas para supuestos art. 49.1	Descripción de las transferencias (encargo) Identificación de los países de destino Identificación de organización internacional La documentación que aporte garantías adecuadas para supuestos art. 49.1

Tabla 45. Cuadro con registros de datos para responsables y encargados.

1.2.3.2. Establecer medidas de protección de datos desde el diseño (Art. 25.1)

Esto supone anticipar la protección de datos al desarrollo del tratamiento que vaya a ser necesario para la puesta en marcha de un producto o servicio. La obligación de que se adopte privacidad desde el diseño recae en el responsable del tratamiento y podrá subcontratar tanto el desarrollo como la implementación de una parte o de la totalidad del tratamiento. Es decir, cuando una empresa de *eHealth* se plantee una idea de negocio donde se vean afectos los datos personales de salud de personas desde el "momento cero" deberán tener en cuenta cómo va a afectar la puesta de ese negocio o proyecto a los derechos y libertades de sus usuarios potenciales o e-pacientes. Un ejemplo de dichas medidas, que se establece de forma expresa en el RGPD, es que el propio tratamiento incorpore: medidas para la seudonimización temprana o, minimización de datos.

1.2.3.3. Fijar medidas de protección de datos por defecto (Art. 25.2).

La idea principal estriba en que *sólo* sean objeto de tratamiento los datos personales que sean *estrictamente necesarios* para cada uno de los fines de tratamiento y en los momentos en que sea estrictamente necesario. Podemos señalar algunas *estrategias básicas* que permiten implementar la privacidad por defecto: (i) *Recogida de datos*: analizar los tipos de datos que se recaban con un criterio de minimización en función de los productos y servicios seleccionados por el usuario; (ii) *tratamiento de los datos:* analizar los procesos asociados a dichos tratamientos para que se acceda a los mínimos datos personales necesarios para ejecutarlos; (iii) *conservación*: implementar

una política de conservación de datos que permita, con un criterio restrictivo, eliminar aquellos datos que no sean estrictamente necesarios; (iv) *accesibilidad:* limitar el acceso por parte de terceros a dichos datos personales.

1.2.3.4. Realizar evaluaciones de impacto (Art. 35 y 36)

Se realizará cuando *sea probable* que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un "*alto riesgo"* para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales[814].

La evaluación de impacto se requerirá en particular en caso de: (i) Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un *tratamiento automatizado*, como la *elaboración de perfiles*, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar; (ii) tratamiento *a gran escala de las categorías especiales* de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o (iii) Observación sistemática a gran escala de una zona de acceso público.

1.5.3.5. Obligación de notificar a la autoridad de control y a los interesados las violaciones o brechas de seguridad (Art. 33 y 34).

Es toda violación de la seguridad que ocasione la *destrucción, pérdida o alteración accidental o ilícita* de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos. El *responsable* ha de notificar la violación de la seguridad, siempre que exista *riesgo* para los derechos y libertadas de las personas físicas, riesgo que ha de ser evaluado por el responsable. El *Comité de Protección de Datos* será el encargado de emitir las guías, recomendaciones

[814] El riesgo en el RGPD tiene varias perspectivas. La primera de ellas es garantizar las *medidas de seguridad* acordes en cada momento al estado de la tecnología y las condiciones específicas de los tratamientos de datos personales. Por otra parte del *enfoque del riesgo para garantizar los derechos y libertades* de las personas se materializa en la protección de datos desde el diseño y las evaluaciones de impacto en la privacidad. Hablamos del "*principio de proactividad"* de los responsables de los tratamientos. Por tanto, las evaluaciones de impacto pueden definirse como un *análisis de riesgos de un producto*, servicio o sistema que aún no existe y se encuentra ligado a los principios de protección de datos desde el diseño y protección de datos por defecto.

o directrices para determinar los niveles de riesgo y las condiciones de la comunicación. En caso de que el *encargado* del tratamiento sufra una violación de seguridad, éste debe notificar sin dilación al *responsable* la existencia de la misma.

El RGPD no indica ni el *formato* de dicha notificación ni el *plazo máximo* para que se realice dicha notificación, ya que el plazo establecido para el responsable se fija a partir del conocimiento de la violación de seguridad. No obstante, la notificación de la brecha a la autoridad de control se ha de producir *antes de las 72 horas,* es decir, en los tres días siguientes al conocimiento por el responsable de la existencia de la violación.

Por otro lado, también hay que *informar* de la política de notificación *a los interesados* que ha establecido el responsable y las razones para implementar la misma en cuanto a si se ha realizado esa notificación, la información revelada, temporización de la información, canales utilizados, nivel de cobertura del conjunto de interesados potencialmente afectados, etc. (Art. 34).

1.2.3.6. Adoptar "códigos tipo" de conducta (Art. 40).

Los códigos de conducta dan respuesta a las necesidades determinados sectores como el de la FarmaIndustria[815] (2009) denominado "Código tipo de Farmaindustria de protección de datos personales en el ámbito de la investigación clínica y de la farmacovigilancia" o su actualización teniendo en cuenta la digitalización del sector y el entorno big data de las investigaciones biomédicas (2017, aún en proceso) que se denominaría "Código de Conducta de protección de datos para la investigación clínica y de la farmacovigilancia"[816].

Por ejemplo, estandarizar los mecanismos para generar confianza a los titulares a la hora de cumplir el *deber de información* (Art. 13) teniendo especial cuidado en los menores de edad, determinar los intereses legítimos según qué contextos, fijar requisitos para la recogida de datos personales; la requisitos para la seudonimización de datos personales; determinar las medidas de seguridad que serán necesarias (art. 25, 25, 32), si

[815] *Supra cit.*

[816] *Supra cit.* El compromiso de los responsables con los códigos se materializa en documentos que permitan la trazabilidad de, por ejemplo, modelos de consentimiento o modelos de cláusulas informativas para los titulares. Quienes serán responsables de promover la elaboración de éstos son los propios Estados miembros, las autoridades de control, el Comité y la Comisión y las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o modificar o ampliar dichos códigos con objeto de especificar cuestiones del propio Reglamento.

podrán existir transferencias internacionales, o los procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento, sin perjuicio de los derechos de los interesados (art. 77 y 79).

En febrero de 2019 se adoptaron y se publicó *las directrices en relación a los códigos tipo de conducta y los cuerpos de monitorización*. El objetivo es proporcionar orientación práctica y ayudar a interpretar el art. 40 y 41 mencionados en aspectos como la presentación, aprobación y publicación de los códigos.

1.2.3.7. Adoptar mecanismos de certificación (Art. 42).

Los mecanismos de certificación también puede ser un recurso para acreditar la *"accountability"* de los responsables[817].

Desde mi punto de vista, falta incentivación "expresa" de los códigos de conducta, certificaciones y sellos en el RGPD. No se saca el suficiente provecho que se esperaba al margen de no establecer obligatoriedad. Por ejemplo, se podría especificar "expresamente" reducciones o exoneración de responsabilidad, incentivos de algún tipo por haberlas adoptado y cumplido.

1.2.3.8.Establecer medidas técnicas y organizativas.

Garantizarán que el tratamiento de datos personales se lleva a cabo de acuerdo con lo previsto en el RGPD y en función del estado de la técnica, los costes que pueden suponer, la naturaleza, el alcance, el contexto y los fines del tratamiento para minimizar el los riesgos que puedan impactar en los derechos y libertades de las personas. No se aconseja que estén enmarcados dentro de una lista o *checklist* inmóvil, sino más bien, que sea resultado de una decisión entre equipos multidisciplinares en el ámbito empresarial.

[817] La certificación siempre implica a un tercero que lleva a cabo la tarea de auditoría sobre un proceso o servicio en los que existe un tratamiento de datos personales y supone un grado de garantía adicional a la diligencia del responsable o del encargado del tratamiento. De igual modo que en el caso anterior, los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de *mecanismos de certificación* en materia de protección de datos y de *sellos y marcas* de protección de datos a fin de demostrar el cumplimiento normativo por parte de responsables y encargados de tratamiento. Estos deberán asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados.

Hemos pasado de un modelo de "listado fijo" (antes del RGPD) con detalle predefinidas basados en función del tipo de ficheros (medidas de seguridad nivel bajo, medio o alto) a un modelo de "listado abierto proporcional al riesgo" de medidas que garantizarán el mejor nivel de seguridad en función de los riesgos detectados en el análisis previos determinado por los propios responsables y encargados. En algunos casos los responsables podrán seguir aplicando las mismas medidas que establece el Reglamento de desarrollo de la antigua LOPD[818] si los resultados del análisis de riesgos previo concluye que las medidas son realmente las más adecuadas para ofrecer un nivel de seguridad adecuado. En ocasiones será necesario completarlas con medidas adicionales o prescindir de alguna de las medidas. El responsable y el encargado del tratamiento (ambos) aplicarán *medidas técnicas y organizativas apropiadas*[819] para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

> a) la pseudonimización y el cifrado de datos personales;
>
> b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
>
> c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
>
> d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

1.2.3.9. Designar un delegado de protección de datos (DPD) (Art.37)

El delegado de protección de datos es la persona encargada informar a la entidad responsable o al encargado del tratamiento sobre sus obligaciones legales *en materia de*

---

[818] BOE. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-2008-979

[819] Según la AEPD, las medidas organizativas son; el deber de información; el deber de confidencialidad y secreto (como por ejemplo, evitar los papeles sobre la mesa, pantallas abiertas, *pen drive* en la basura), y la formación (Ver; https://www.eldiario.es/sociedad/delito_de_revelacion_de_secretos_0_854965182.html), en definitiva; los derechos titulares; las violaciones de seguridad de datos personales. Y las medidas técnicas podrían ser; la identificación de usuarios; el deber de salvaguarda: la actualización de ordenadores y dispositivos; malware; cortafuegos o firewall; cifrado de datos; copia de seguridad; control de acceso a los datos (es decir, cada empleado accederá a los datos que son estrictamente necesarios para su trabajo); identificación y autentificación de todos los usuarios que tengan acceso a la base de datos; registro de actividades del tratamiento; cifrado de soportes; seudonimización; minimización de los datos; procedimientos de copias de seguridad; confección de los avisos legales en el que el consentimiento se preste según nuevo Reglamento y actualización de los derechos de los interesados.

protección de datos, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la autoridad de control y actuar como punto de contacto entre ésta y la entidad responsable del tratamiento de datos[820]. E incluso hay quien sostiene que podría tener papel de "mediador"[821].

Deberá designarse si (a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial; (b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o (c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10 *(Art. 37 RGPD).*

---

[820] Las funciones que señala el RGPD son: *(i) Función de información y supervisión.* Debe informar y asesorar al responsable o al encargado del tratamiento de las obligaciones normativas en protección de datos que les incumban. Por tanto, se exige una formación en privacidad muy cualificada por parte del DPO, tal y como señala, además del sentido común, el articulo 37.5 del RGPD. Además deberá asesorar al responsable o al encargado del tratamiento acerca de la evaluación de impacto relativa a la protección de datos (también es responsable de supervisar su realización). Debe informar y asesorar a los empleados que traten datos personales en el seno de las organizaciones responsables o encargadas del tratamiento. A tal fin debería existir un canal interno, ya sea a través de la *intranet* corporativa, o a través de un buzón interno de consultas. *(ii). Función de supervisión del cumplimiento normativo.* Debe supervisar el adecuado cumplimiento de las normas sobre protección de datos en la entidad u organización. Debe revisar las políticas internas de privacidad en la organización y su adecuación normativa. También deberá asignar responsabilidades entre los miembros de la organización, respecto a las obligaciones en materia de protección de datos. Se debe ocupar de la realización de acciones internas de concienciación respecto al cumplimiento efectivo de las normas sobre privacidad, incluidas las de carácter interno. Además, debe realizar acciones formativas para el personal que participa en las operaciones de tratamiento de datos. Debe supervisar las evaluaciones de impacto en la protección de datos. El Dictamen del GT29 referido ut supra, destaca que su función se convierte, al mismo tiempo, en un deber en cuanto a «ofrecer el asesoramiento que se le solicite» y «supervisar» la aplicación de dicha evaluación. El Dictamen WP 243 recomienda que el asesoramiento del DPO se extienda, entre otras cuestiones, a determinar la metodología a seguir, o si se debe externalizar o no la elaboración de la evaluación de impacto. (iii) *Función de cooperación y enlace con la autoridad de control.* Debe cooperar con la autoridad de control, o agencia de protección de datos correspondiente. También deberá actuar como punto de contacto de la Agencia para las cuestiones relacionadas con el tratamiento de datos personales incluida la consulta previa (que se detalla en el artículo 36 del RGPD respecto a evaluaciones de impacto que muestren alto riesgo para la privacidad), y consultar en su caso, sobre cualquier otro asunto. (iv) *Función de atención a los interesados.* Debe atender a los interesados que lo soliciten. Al respecto, el artículo 38.4 del RGPD indica que «los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos».

[821] Cfr. Adsuara, B. (31 de enero de 2019). ¿Y por qué no una Mediación en Protección de Datos? La Información. Recuperado de https://www.lainformacion.com/opinion/borja-adsuara/y-por-que-no-una-mediacion-en-proteccion-de-datos/6491255/

Conforme a la LOPDGDD, en concreto a su art. 34, los centros sanitarios, aseguradoras y reaseguradoras y los prestadores SSI, entre otros, necesitarán esta figura obligatoriamente.

1.2.4. Legitimación del tratamiento de datos personales de salud

El punto de partida para el tratamiento de datos personales es determinar la base jurídica que permite realizar lícitamente las distintas operaciones de tratamiento. Como ya hemos dicho en el apartado anterior, el tratamiento se considera lícito si se da alguna de las siguientes condiciones:

i. *Consentimiento*. Se exige además que sea explícito para los datos pertenecientes a las *categorías especiales* como son los datos de salud y los datos genéticos o biométricos (artículo 9.2,a). Desaparece el consentimiento tácito, no se permiten las *casillas premarcadas* y si se presta el consentimiento para varios fines, este deberá prestarse para cada uno de ellos (asistencia sanitaria, investigación agencias públicas o laboratorios farmacéuticos privados). Si el consentimiento recabado con anterioridad cumple los criterios del RGPD no es necesario recogerlo de nuevo. El responsable del tratamiento deberá demostrar la validez del consentimiento y éste puede ser revocable, por lo que se tiene que informar de este hecho.

ii. *Relación contractual.* El RGPD no se desarrolla mucho esta base, limitándose a establecer en su artículo 6.1b), que será licito el tratamiento "necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales". En los contratos de prestación de servicios se deberán adaptar a lo que dispone el RGPD para que el tratamiento de los datos personales sea conforme a derecho.

iii. *Interés vital.* Aunque el RGPD no incluye una definición, el Considerando 46 se refiere a "un interés para la vida del interesado o de otra persona" y añade que solamente se puede legitimar el tratamiento sobre la base del interés vital cundo no se pueda basar en otra base jurídica diferente señalando como ejemplos tratamientos necesarios para fines humanitarios, incluido el control de epidemias o situaciones de emergencia humanitaria[822].

iv. *Interés legítimo.* El artículo 9.2.d RGPD, donde se incluye elenco de excepciones al tratamiento de datos de categoría especial como son los datos de salud, no se encuentra el interés legítimo dentro del mismo. Este precepto se refiere a casos cuando el tratamiento es efectuado por una "fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se

[822] En circunstancias excepcionales, puntuales y urgentes podría invocarse el interés vital como base jurídica del tratamiento. Podría ser de aplicación respecto del tratamiento de datos de salud para *la prestación de asistencia sanitaria por profesionales sanitarios sujetos al secreto profesional* o por otra persona sujeta a una obligación equivalente de secreto, para la prevención, diagnóstico, prestación de asistencia o tratamientos sanitarios o la gestión de servicios sanitarios.

comuniquen fuera de ellos sin el consentimiento de los interesados". Si tenemos en cuenta dicha circunstancia, encontrar su aplicación en el objeto de estudio de nuestro trabajo puede resultar bastante complicado.

Con esta acotación expresa de la utilización del interés legítimo como base legal destinado a asociaciones sin ánimo de lucro, el legislador pretende reforzar los derechos de los titulares de datos frente a aquellos responsable (con ánimo de lucro) que pudieran caer en la tentación de "utilizarla" como opción "de todo vale", aunque no sería para nada así, puesto que requiere (de igual forma) de "*accountability*" y de un juicio de ponderación (Guerrero, 2018)[823]. Como el autor señala, se informa del tratamiento, de esta base legitimadora, qué interés legítimo se produce, la justificación de porque puede prevalecer el interés legítimo sobre el derecho fundamental y de las medidas para mitigar los riesgos. De lo contrario podría "darse la paradoja de que los datos de los interesados acabaran siendo menos protegidos por el hecho de que concurrieran datos "especiales"**.** Él se apoya además en el *informe (wp217) del GT29 de 2014 sobre interés legítimo*. Los artículos del artículo 6 –legitimación- y 9 -datos de categoría especial- del Reglamento no se aplican de forma excluyente sino conjuntamente, lo que significa que deberían tener una legitimación los datos de salud; "En este sentido, la aplicabilidad de las excepciones del artículo 8 no excluye la aplicabilidad de los requisitos del artículo 7 (el consentimiento), y ambos, cuando así proceda, deberán aplicarse acumulativamente".

Es más, el *informe del GT29 de 2017 sobre profiling y decisiones* completamente automatizada**s** (wp251) específica claramente el art.9 "los responsables del tratamiento solo pueden tratar datos personales de categoría especial si se cumplen *una* de las condiciones previstas en el art.9, apartado 2 (por ejemplo, el consentimiento o la relación contractual, como señala el legislador "el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado";) así como *una* condición del artículo 6 (por ejemplo, *6.1.f* "cuando el tratamiento es necesario para la *satisfacción de intereses legítimos perseguidos por el responsable* del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño" o por ejemplo, *6.1.j.;* "el tratamiento es necesario con fines de archivo en interés público*, fines de investigación científica* o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, *sobre la base del Derecho de la Unión o de los Estados miembros*, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.".)

v. *Tratamientos necesarios para el cumplimento de una obligación legal o para el cumplimento de una misión realizada en interés público o en el ejercicio de poderes públicos.* Es la base jurídica para el tratamiento de datos personales por parte de las Administraciones Públicas, y por tanto la

[823] García Herrero, J. (16 de julio de 2018). Sí se puede! Datos de categoría especial tratados sobre interés legítimo.Recuperado de https://jorgegarciaherrero.com/datos-de-categoria-especial-tratados-sobre-interes-legitimo/

legitimación del tratamiento de los datos relativos a la salud para la asistencia sanitaria por los centros del Sistema Nacional de Salud, en esta red de centros comprenden los centros de titularidad pública y los de titularidad privada que mediante concierto u otra habilitación legal y cumpliendo todas las normas exigidas en materia de protección de datos y confidencialidad, prestan asistencia a una población determinada, (el considerando 45 del RGPD recoge la legitimación de personas de Derecho privado para el cumplimiento de misiones de interés público en fines sanitarios como la gestión de los servicios públicos).

3.2.3.1. Ejemplo real de finalidades y legitimación del tratamiento de responsable del tratamiento de datos personales ("Aseguradora de salud digitales"[824]).

	Finalidades	**Legitimación**
a.	Formalización, desarrollo y ejecución del contrato	Ejecución del contrato de prestación de servicios.
b.	Prestación del servicio asistencial integral objeto del Contrato	Ejecución del contrato de prestación de servicios.
c.	Gestionar el acceso y uso de la herramienta del portal del Centro Médico (el "Portal")	consentimiento
d.	Cesión de los Datos Personales a las Empresas del Grupo para la investigación científica y para el diseño, mejora u ofrecimiento de modelos asistenciales objeto del Contrato.	Ejecución del contrato de prestación de servicios.
e.	Prestación del servicio de video-consulta u otros por parte de Sanitas	Ejecución del contrato de prestación de servicios.
f.	Cumplimiento de obligaciones que le correspondan a Sanitas por mandato legal.	cumplimiento de una obligación legal aplicable al responsable (aseguradora)
g.	Ceder Datos Personales a Empresas del Grupo con el fin de elaborar perfiles	consentimiento
h.	Elaboración de perfiles para el ofrecimiento de nuevos productos y servicios.	satisfacción del interés legítimo
i.	Envío de comunicaciones comerciales por cualquier canal, incluido por vía electrónica	consentimiento
j.	Procedimientos de anonimización y pseudoanonimización	la necesidad del tratamiento para fines de investigación científica o estadística
k.	Ceder Datos Personales a Empresas del Grupo con fines de investigación científica y/o estadística para fines comerciales	consentimiento
l.	Ceder Datos Personales a terceros	consentimiento

Tabla 46. Ejemplo real de finalidades y legitimación del tratamiento de responsable del tratamiento de datos personales de Aseguradora de salud digitales. (contenido Página web)

3.2.3.2. Ejemplos de encargos del tratamiento y cesiones

Encargados de tratamiento	**Cesionario de datos**

[824] Vid. https://www.sanitas.es/contratacionservicios/textoLegal?mostrarFancyPoliticaPrivacidad#terceraspartes_hospitales

Servicios médicos y de consultoría asistencial.	Empresas del grupo de la aseguradora.
Servicios fisioterapia, psicología y terapia, servicios protésicos, sanitarios.	Centros sanitarios.
Centros de radiología y laboratorios médicos externos.	Servicios protésicos.
Actividades auxiliares a los servicios hospitalarios.	Centros de radiología y laboratorios médicos externos al centro.
Servicios de telecomunicaciones.	Mutualidades y compañías de seguros.
Servicios de auditoría y consultoría.	Mutuas de accidentes profesionales.
Servicios financieros y servicios bancarios.	Empresas de vigilancia de la salud.
Servicios de formación.	Subcontratas de empleados.
Servicios de tercero de confianza	Empresas colaboradoras para la promoción de productos y servicios.
Servicios de *"call center"*	Servicios sociales y otros Organismos públicos.
Servicios de encuesta de calidad	AAPP, AEAT, Tribunales y otras autoridades
Servicios postales, de distribución y de mensajería	Personas físicas o jurídicas a las que sea necesario comunicar por obligación legal
Servicios de seguridad física	
Servicios de *mailing*, impresión y ensobrado	
Servicios de archivo, custodia, almacenamiento y digitalización.	
Servicios de retirada y destrucción de documentación.	
Servicios de "backoffice"	
Servicios administrativos	
Servicios de publicidad y comunicación	
Servicios de actividades jurídicas y reclamaciones	
Servicios de gestión y recuperación de cobros	
Servicios de prevención y mutuas	
Servicios de mantenimiento	
Servicios informáticos	
Servicios de plataformas tecnológicas	
Servicios de *hosting*	
Servicios de procesos de datos	
Servicios de arquitectura e ingeniera	
Servicios de "backup"	
Servicios de continuidad de negocio	
Servicios de custodia electrónica	
Servicios de consultoría informática	
Servicios de seguridad y ciberseguridad	
Otros servicios relacionados con las tecnologías de la información y la informática	

Tabla 47. Ejemplos de encargos del tratamiento y cesiones Fuente: Sanitas (contenido Página web)

1.2.5. Tratamiento de categorías especiales de datos y ámbito de salud.

El RGPD incluye en el concepto de categorías especiales de datos los denominados datos especialmente protegidos en la antigua LOPD como son las opiniones políticas; las convicciones religiosas o filosóficas; la afiliación sindical; los que revelen el origen racial o étnico; *los relativos a la salud;* a la vida u orientación sexual de una persona. Pero además incorpora nuevas categorías de datos como son los *datos genéticos y los datos biométricos.*

La profesora Pilar Nicolás (2018)[825] entiende que es preferible referirnos a "*contextos y finalidades* del tratamiento de datos" que de "categorías de datos", *per se*. En este sentido, ella se cuestiona si la información personal afecta a la salud de una persona que es fumadora podría entenderse como tal información, un dato personal (*per se)* . Para la profesora, "es más importante hablar de "*datos con fines sanitarios"* que utilizar el concepto *"dato de salud*".

Ahora bien, volviendo al RGPD, la regla general contemplada es la *prohibición del tratamiento de categorías especiales* de datos (art. 9.1). No obstante, se recoge un amplio abanico de *excepciones* (art. 9.2) a esta regla general, como por ejemplo, que los tratamientos tengan como finalidad la medicina preventiva o laboral, la evaluación de la capacidad, la evaluación de la capacidad laboral del trabajador, el diagnóstico médico, la prestación de asistencia o el tratamiento de tipo sanitario o social, o la gestión de los sistemas y los servicios de asistencia sanitaria y social.

Por lo tanto, los *datos de salud siguen siendo categorías especiales*[826] en el Reglamento donde la regla general establece una prohibición para estos datos y a diferencia del resto de tipos de datos, donde las bases jurídicas operan por igual, en este tipo de categorías de datos opera un *consentimiento reforzado* **(**ley ensayos clínicos, ley investigación biomédica).

---

[825] Nicolás, P. *Congreso Big Data biosanitarios: Oportunidades e implicaciones jurídicas*. G.I. Cátedra de Derecho y Genoma Humano. Universidad del País Vasco UPV/EHU,8 y 9 de octubre de 2018.
(Se señaló que "las fuentes son variadas, como por ejemplo, las fuentes de información clínica, proyectos de investigación, o las redes de diagnóstico de enfermedades comunitarias. por lo que no podrían ser encasillados independientemente").

[826] Por su parte, el considerando 53 hace las siguientes aclaraciones: "Las categorías especiales de datos personales que merecen mayor protección únicamente deben tratarse con fines relacionados con la salud cuando sea necesario para lograr dichos fines en beneficio de las personas físicas y de la sociedad en su conjunto, en particular en el contexto de *la gestión de los servicios y sistemas sanitarios o de protección social*, incluido el tratamiento de esos datos por las *autoridades gestoras de la sanidad y las autoridades sanitarias nacionales* centrales con fines de control de calidad, gestión de la información y supervisión general nacional y local del sistema sanitario o de protección social, y garantía de la continuidad de la asistencia sanitaria o la protección social y la asistencia sanitaria transfronteriza o fines de seguridad, supervisión y alerta sanitaria, o con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, basados en el Derecho de la Unión o del Estado miembro que ha de cumplir un objetivo de interés público, así como para estudios realizados en interés público en el ámbito de la salud pública. Por tanto, el presente Reglamento debe establecer condiciones armonizadas para el tratamiento de categorías especiales de datos personales relativos a la salud, en relación con necesidades específicas, en particular si el tratamiento de esos datos lo realizan, con fines relacionados con la salud, personas sujetas a la *obligación legal de secreto profesional.* El Derecho de la Unión o de los Estados miembros debe establecer medidas específicas y adecuadas para proteger los derechos fundamentales y los datos personales de las personas físicas. Los Estados miembros deben estar facultados para mantener o introducir otras condiciones, incluidas limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud. No obstante, esto no ha de suponer un obstáculo para la libre circulación de datos personales dentro de la Unión cuando tales condiciones se apliquen al tratamiento transfronterizo de esos datos".

Pero hay una *excepción a esta prohibición que se encuentra al tratamiento de datos con fines de investigación científica* (art. 89 RGPD). La legitimación estará en el reconocimiento de un interés público relevante reconocido en una norma. Abordaremos la cuestión de investigación científica en el apartado correspondiente y a lo largo de este capítulo. En definitiva, el nuevo Reglamento regula de una manera más detallada, y se puede decir también que se produce una ampliación o extensión de las posibilidades de tratamientos de datos relacionados con la salud, sobre todo *sin consentimiento del titular de derechos*.

Pero antes de avanzar, detengámonos en las excepciones relativas al ámbito de la salud y en sus afecciones.

En concreto, nos referimos a las excepciones señaladas en el RGPD, que son las siguientes:

> a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales *con uno o más de los fines especificados*, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;
>
> b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del *Derecho laboral y de la seguridad y protección social,* en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;
>
> c) el tratamiento es necesario para *proteger intereses vitales* del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;
>
> d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin *ánimo de lucro*, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;
>
> e) el tratamiento se refiere a datos personales que el interesado ha hecho *manifiestamente públicos;*
>
> f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su *función judicial;*

g) el tratamiento es necesario por razones de un *interés público* esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado

h) el tratamiento es necesario para fines *de medicina preventiva o laboral*, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario por razones de *interés público en el ámbito de la salud pública*, como la protección frente a amenazas transfronterizas graves para la salud, o para *garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios*, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional

j) el tratamiento es necesario con *fines de archivo en interés público*, fines de *investigación científica* o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado".

Respecto a la excepción relativa al tratamiento de los datos de salud en el ámbito de la *asistencia sanitaria*, vemos que se sigue disponiendo la necesidad de que se traten por un profesional sujeto a la obligación de secreto, pero se amplían los fines para los que es posible su tratamiento (art. 9.2.h y 3) al igual que de la idea tradicional de que se pueden tratar los datos de salud para la asistencia sanitaria al paciente (prevención, diagnóstico, etc.) o la gestión de la asistencia sanitaria, pasamos a la posibilidad de tratamiento con fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social. Por tanto, nos encontramos con una idea de asistencia y gestión se expande y se adapta a la nueva realidad, teniendo en cuenta el ámbito de la medicina, también en el importante ámbito laboral o el tratamiento de datos de salud en el marco del tratamiento y asistencia social.

Respecto a la importante excepción de *interés público* (recogida también en Directiva y que además ha sido base jurídica para el tratamiento de datos de salud todo este tiempo), el Reglamento la mantiene con los requisitos que señala en el apartado 2.g del art. 9).

Y para finalizar, el legislador, incorpora dos nuevas excepciones relacionadas con el mencionado interés público (art. 9.2.i y j) que señalaba la propia Directiva. Nos referimos al interés público en el *ámbito de la salud pública* para cuestiones relacionadas con riesgos serios de sanidad transfronterizos, o para garantizar altos niveles de calidad de seguridad de asistencia y medicamentos o productos o con el tratamiento con fines de investigación científica, por ejemplo. [827]

Por tanto, las excepciones previstas en el ámbito de la sanidad incluyen las relacionadas con garantizar la calidad y la rentabilidad de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el *régimen del seguro de enfermedad* o con fines de archivo en interés público, fines *de investigación científica* e histórica o fines estadísticos (que veremos en el apartado correspondiente).

Respecto al *régimen de seguro de enfermedad,* una vez más la traducción del inglés del RGPD al español hace debilitar la precisión conceptual. Siguiendo esta concepción, en mi humilde opinión, puedo entender una definición contenida en la *Ley del Seguro Obligatorio*[828] del año 1942 para clarificar el contexto y el sentido de los tratamientos de datos que gozan de las excepciones citadas en el RGPD. Para entender, mejor el

[827] El considerando 52 hace algunas aclaraciones: "Asimismo deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones y con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud. Tal excepción es posible para fines en el ámbito de la salud, incluidas la *sanidad pública y la gestión de los servicios de asistencia sanitaria*, especialmente *con el fin de garantizar la calidad y la rentabilidad de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, o con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos*. Debe autorizarse asimismo a título excepcional el tratamiento de dichos datos personales cuando sea necesario para la formulación, *el ejercicio o la defensa de reclamaciones*, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial".

[828] Cuyos fines eran: "a) La prestación de asistencia sanitaria en caso de enfermedad; b) la prestación de asistencia sanitaria en caso de maternidad. c) la indemnización económica por la pérdida de retribución sufrida por el asegurado y derivada de los riesgos determinados en el apartado a. de este articulo; d) las indemnizaciones en caso de maternidad; e) la indemnización por gastos funerarios al fallecer el asegurado; f) la práctica de las funciones de medicina preventiva que le correspondan". En todo caso, tenemos que tener claro que las excepciones se conjugarían en el ámbito de la sanidad pública teniendo en cuenta todo lo dispuesto anteriormente y lo establecido en el RGPD".
Mas info en Boletín Oficial Español. https://www.boe.es/datos/pdfs/BOE//1943/332/A11427-11436.pdf

sistema de seguro de sanidad, sus actividades (y por ende, los tratamientos de datos posibles).[829]

Las excepciones estarán dirigidas a la *gestión de los servicios y sistemas sanitarios o de protección social.* Pero, ¿a qué se refiere el legislador con el término "gestión de servicios y sistemas sanitarios"? Los sistemas sanitarios son "las organizaciones que prestan servicios sanitarios como hospitales, centros de salud, funcionarios profesionales y servicios de salud pública, así como sectores, instituciones y organizaciones (privadas) cuyo objetivo último es la salud. Otra definición que podremos encontrarnos –también a lo largo de este trabajo- es el de "proveedores de salud" refiriéndose tanto a salud pública como a salud privada. Una definición muy adecuada para "sistemas sanitarios" es la de *Javier Cabo*[830] quien establece que son "son un complejo entramado de relaciones entre distintos agentes, unos agentes que podemos enumerar de manera fundamental como los gobiernos, los ciudadanos, las aseguradoras y los proveedores de servicios sanitarios (…)". Pero si algo diferencia los servicios sanitarios de otros son una serie de características como producidos y consumidos en el momento, son personalizados y producidos por demanda, no pueden ser "reciclados o reprocesados", no se pueden ensayar, no pueden eliminarse después de

---

[829] Cabo Salvador, J. *Los sistemas sanitarios y sus objetivos.* Udima. Recuperado de https://www.gestion-sanitaria.com/1-sistemas-sanitarios-objetivos.html.

Podríamos señalar la siguiente clasificación de sistemas de financiación sanitaria de *Javier Cabo*: (i) *Sistema del Estado de bienestar*. Se encuentra incluido el sistema sanitario español (el de R.U. o países nórdicos, también), son los sistemas englobados en lo que se conoce como SNS, que son financiados por impuestos donde no es posible estar exento de la financiación. Aunque se trata de un acceso universal y gratuito, en algunas prestaciones se requiere del copago o pago adicional. Están bajo control estatal.(ii) *Seguridad Social.* Está asociado a la retención de parte de los ingresos de los trabajadores. Estas cuotas constituyen un fondo específico sólo para la prestación asistencial de aquellos colectivos que cotizan trabajadores y sus familias. Es independiente a otros ingresos del gobierno. Está implantado en Latinoamérica, Francia, Suiza. Hay algo muy interesante en este sistema, y es que "habitualmente, permite la elección de asegurador o proveedor sanitario, lo que incorpora variables de competitividad entre ellos y, de manera indirecta, facilita la satisfacción de los usuarios con los servicios". "No disfruta del carácter universal de los SNS y tiene unos costes de administración más altos y complicados de gestionar y adicionalmente, al ser parte de los costes laborales, puede limitar o disminuir la competitividad de las empresas". (iii) *Aseguramiento voluntario privado y pago directo de los servicios.* La participación depende de la decisión individual bien por el aseguramiento voluntario o por el pago directo de los servicios, y en estrecha relación con la capacidad de pago de que disponen. está sujeta al riesgo de la selección adversa ya que pueden quedar excluidos del aseguramiento por no encontrar quien cubra su riesgo o no disponer de suficiente nivel económico para soportar el coste de la póliza.

[830] *Ibídem.*

ejecutarse, son intangibles, etc. Y por ello la gestión[831] y los tratamientos de datos personales serán particulares y con sus características propias. ¿A qué se referiría el legislador con el término *las "autoridades sanitarias nacionales*" o "*autoridades gestoras de la sanidad?* Entendemos que se referirán a las administraciones públicas competentes correspondientes. El ex director general de sanidad de hace más de dos décadas ya preveía una evolución futura en las mismas tendente a una dependencia, tendrán una creciente dependencia e influencia de instancias internacionales[832] (científico-asesor, en el caso de la OMS, añadiría, por ejemplo el Comité Internacional de Bioética o, de tipo ejecutivo, como la propia UE). Desde mi opinión destacaba como característica principal de las autoridades sanitarias: la necesidad de contar con "una prístina definición jurídica de sus *obligaciones y de los procedimientos* para cumplir". Aunque el autor se refiera en el ámbito general de ejecución de asistencia sanitaria (errores médicos, consentimientos informados, etc.,) las obligaciones y los procedimientos conforme al ecosistema regulatorio, deberían alcanzar a la protección de datos personales y la gestión de la información sanitaria, donde la Directiva del 95 ya iba sentando las bases de un nuevo paradigma de los derechos y libertades de las personas, ciudadanos y pacientes de la UE. Resulta interesante la afirmación del autor (habida cuenta el momento de la declaración) en la que establece que: "la técnica jurídica deberá desarrollar un cuerpo doctrinal en el que se determine con claridad en qué ocasiones las autoridades sanitarias, siguiendo un gradiente de más a menos intervención sobre las libertades individuales, tienen que obligar, cuando prohibir, cuando limitar, cuando aconsejar, cuando advertir, cuando informar y cuando no intervenir en absoluto". De hecho añadía, que "no es descabellado imaginarse un futuro en el que se deba proceder a una oficial catalogación de los *riesgos*, en función de su gravedad y evidencia. Para ese momento, será bueno que se tenga construido el instrumento jurídico necesario que, sin duda, deberá estar inspirado en una previa

---

[831] Así por ejemplo, según Javier Cabo, "el conjunto de actividades y funciones que los directivos sanitarios deben ejercer recorre un amplio abanico que va desde la elaboración, ejecución y seguimiento del presupuesto, la gestión de los recursos humanos, la contratación de personal, la mediación en conflictos de distinto origen (sindical, interprofesional, departamentos clínicos, proveedores…), la atención y resolución de reclamaciones de usuarios, la ejecución de los programas docentes y de investigación, la asignación de recursos, la elección de tecnología, el seguimiento de los contratos y los fallos de los proveedores, y un largo etcétera, que se podría resumir en dos acciones concretas: tomar decisiones adecuadas y resolver problemas".

[832] Cfr. Polledo, J.J.F. (Septiembre 1997). El papel de las autoridades sanitarias ante los retos de la salud pública del S. XXI. Revista Española de Salud Pública. Vol. 71. No. 5. Madrid. Recuperado de http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1135-57271997000500001

reflexión ética que, de momento, se echa de menos en el campo de la salud pública". Llama la atención los términos "riesgos" y "reflexión ética", conceptos que salen a la luz de manera muy frecuente en los debates jurídico-tecnológicos de la actualidad también refiriéndose al ámbito de la salud. Acaso, ¿ya se podía intuir que la "técnica jurídica" se enfocaría a la gestión de riesgos que pueden afectar a los derechos y libertades de las personas? ¿o se podría venir que el contexto tecno-sanitario y de asistencia social iría evolucionando paralelamente iban irrumpiendo tecnologías en el S.XXI?

1.2.6. Derechos de los titulares de datos personales de salud

En primer lugar, hay que tener en cuenta que no solo serán titulares de datos personales los "e-pacientes"[833] (de sanidad pública o privada) sino también en general los "consumidores" de la industria del cuidado de la salud digital pero a su vez todos ellos son considerados "ciudadanos". La nueva normativa, sin duda, viene a otorgar más poder al titular incorporando nuevos derechos y hace referencia a las normas sectoriales de Sanidad e Investigación como la Ley de autonomía del paciente (Ley 41/2002), la Ley General de Sanidad (Ley 14/1986) o la Ley de Investigación Biomédica (Ley 14/2007).

Nos referimos a:

i. *El derecho de acceso*[834]. Es el derecho del interesado a obtener información sobre sus datos en el ámbito de la asistencia sanitaria, como por ejemplo, el acceso al historial clínico electrónico (HCE) del que hemos hablado en el punto 2.3. de este capítulo. En este ámbito de la asistencia sanitaria, se señala el interesado tiene

[833] Podríamos denominar a e-paciente a toda persona física que recibe los servicios y cuidados en materia de asistencia médica, o de bienestar o estética en un entorno digital o virtual como consecuencia de un contrato de prestación de servicios o en el marco de la relación con la Sanidad pública.

[834] En este sentido, *Elisa Debíes* (2017) señala que "la Cnil (la Autoridad francesa de protección de datos) pretende establecer en Francia (quizás se puede referir a la Ley n° 2016-41 du 26 janvier 2016, de modernisation de notre système de santé), el equivalente el *"Blue Button"* estadounidense, que permite desde 2010 a más de 150 millones de americanos de acceder a sus datos médicos personales a través de un único enlace. Reino Unido ya ha anunciado el mismo servicio para el 2018. Concretamente se trata de dar al ciudadano acceso a sus datos de salud y bienestar en un formato que las maquinas puedan leer, para poder interpretarlos, definir usos elegidos y controlados por el mismo ciudadano, combinándolos con otros datos o utilizando servicios terceros. Estos datos provienen de documentos pdf, sitios web, aplicaciones, objetos conectados, etc.". Para más info: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000031912641&categorieLien=id

derecho a "conocer y obtener copia de la Historia Cínica (Art. 15.3 RGPD y art. 18.1. Ley de autonomía del paciente)[835][836].

ii. *El derecho de rectificación.* El responsable de tratamiento debe rectificar aquellos datos que estén incompletos o sean inexactos. Se justifica este derecho por el principio de calidad de los datos, que deben ser veraces, actuales y puestos al día y exactos. Esto coincide con lo que establece la Ley de autonomía del paciente (Art. 15) exige que la historia clínica tenga *información veraz y actualizada* del estado de la salud del paciente. Cuando hablamos de historia clínica nos referimos -y se extiende- también al Historial clínico electrónico (HCE) y a registros electrónicos que contienen datos personales de salud.

iii. *El derecho de oposición.* El interesado se puede oponer al tratamiento de los datos personales por motivos relacionados con su situación particular. Ahora bien, ¿el responsable del tratamiento, por ejemplo, un hospital independiente o un consorcio de universidades investigadoras, centros médicos y empresas farmacéuticas participantes en un entorno DLT/*blockchain*, podrían denegar el ejercicio de este derecho alegando motivos legítimos imperiosos para que el tratamiento prevalezca sobre el interés del solicitante o para el ejercicio o defensa de reclamaciones?. Así por ejemplo, en aseguradoras como *Sanitas*[837] se puede leer en políticas de privacidad lo siguiente: "en principio, está obligado (el paciente) a proporcionar todos los datos que le solicita Sanitas, no obstante, si no se facilitan todos los datos personales considerados necesarios para, entre otros, procurarle la máxima asistencia sanitaria que pueda precisar, ello puede ocasionar un retraso o impedir su diagnóstico o tratamiento". El legislador comunitario en el RGPD (art. 21.6) reconoce expresamente este derecho para tratamiento *con fines de investigación científica* o

[835]Es de destacar que no se incluye el derecho de acceso a datos de terceros que constan en la Historia Clínica y tampoco a los *comentarios y anotaciones subjetivas* de los profesionales (artículo 15, 4 RGPD y articulo 18,3 Ley 41/2002). Quizás resulta más difícil de encontrar esta salvedad en eHealth por cuestiones técnicas pero posiblemente puede darse alguna analogía en función del software sanitario y tecnología/s empleada/s.

[836] Me parecería interesante resaltar que no se contempla incluido en este derecho, el conocer *quien* ha accedido a la Historia Clínica como ocurre en la Ley francesa de Modernización del Sistema de Sanidad (2016): "Art. L. 1111-19.- El titular del titular accede directamente, por medios electrónicos, al contenido de su archivo. "También puede acceder a la lista de profesionales que tienen acceso a su registro médico compartido. Puede, en cualquier momento, modificarlo. Por otro lado , cada vez más *plataformas de blockchain/DLT* aplicada a la salud y aplicadas a la modernización de los sistemas de sanidad pública como en Suiza o Estonia ponen el foco en esta cuestión. Posibilidad que no se habría planteado el legislador comunitario lo que evidencia una vez más como la tecnología se adelanta al desarrollo de legislaciones

[837]Vid. SANITAS, https://www.sanitas.es/contratacionservicios/textoLegal?mostrarFancyPoliticaPrivacidad (Pto. I)

estadístico salvo que sea un tratamiento de datos por interés público. Es el caso de que el interesado titular de datos personales no le interese que sus datos sean tratados con el fin de investigación.

iv. *El derecho de supresión* de datos personales sin dilación cuando exista tratamiento ilícito o desapareció el motivo del mismo. Este es el derecho que más controversia puede despertar en el ámbito de la salud.

v.1. El derecho de supresión en el ámbito de la asistencia sanitaria.

Existen algunas excepciones debido a los plazos de obligación legal de conservación, otras obligaciones de conservación y el derecho de asistencia sanitaria del paciente. El plazo mínimo está contenido en el art. 17.1 de la Ley de autonomía del paciente y marca que será "como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial". Pero además en el propio RGPD (art. 17.3) señala que se aplicará cuando el tratamiento sea necesario para, el cumplimento de un misión realizada en interés público o en el ejercicio de poderes públicos, por interés público en el ámbito de la salud pública, cuando se trate con fines de investigación científica o estadística en la medida que el ejercicio del derecho de supresión pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento o para el ejercicio o defensa de reclamaciones. Por su parte, la LOPDGDD, recoge la *obligación de bloqueo de los datos* cuando se realicen operaciones de rectificación o supresión, quedando a disposición exclusiva de los jueces y tribunales, Ministerio Fiscal o Administraciones Públicas competentes, para la exigencia de responsabilidades derivadas del tratamiento y por el plazo de prescripción de las mismas. Existe la obligación de contestar siempre, aunque sea denegándolo de forma motivada y en un plazo de 1 mes desde la solicitud.

v.2. El derecho de supresión (o "derecho de olvido"[838]) en *e-Health*

Según la AEPD[839], "es la manifestación del derecho de supresión aplicado a los buscadores de internet" y "hace referencia al derecho a impedir la difusión de

[838] El Tribunal de Justicia de la Unión Europea (TJUE) hizo pública el 13 de mayo de 2014 una sentencia que establece, como ya venía aplicando la Agencia en sus resoluciones, que el tratamiento de datos que realizan los motores de búsqueda está sometido a las normas de protección de datos de la Unión Europea y que las personas tienen derecho a solicitar, bajo ciertas condiciones, que los enlaces a sus datos personales no figuren en los resultados de una búsqueda en internet realizada por su nombre. Para ver sentencia: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES

información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa" [840]. Por ejemplo, se incumpliría la normativa cuando no se permitiera ejercer este derecho ante la información personal indexada por motores de búsqueda a través en plataformas de foros de salud (tipo "*patients like me"*),o a través de información añadida de forma voluntaria o a través de información publicada (nombre, apellidos, fotografía, varios datos de salud) de forma voluntaria con dispositivos IoT en plataformas sociales *("Social Diabetes")* como el siguiente caso susceptible de acabar indexado en motores de búsqueda o en base de datos de aseguradoras de salud.

v. *El derecho a la portabilidad.* Es el derecho a recibir los datos a solicitud del interesado, en un formato estructurado, de uso común y lectura mecánica, con la intención de transmitirlos a otro responsable de tratamiento, cuando el tratamiento está basado en un contrato o en el consentimiento y se efectúe por medios automatizados. Es importante resaltar que no es aplicable para la sanidad públicas (Administraciones Públicas): "tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en

[839] Cfr. https://www.aepd.es/areas/internet/derecho-al-olvido.html

[840] En 2019, el Abogado General Szpunar propuso al TJUE que declare que los gestores de motores de búsqueda deben aceptar sistemáticamente las solicitudes de *desreferenciación de datos sensibles*, aunque garantizando la protección del derecho de acceso a la información y del derecho a la libertad de expresión. Este sería un buen paso hacia el derecho del "olvido" de los datos personales sensibles como los de la sexualidad. Tribunal de Justicia de la Unión Europea, COMUNICADO DE PRENSA n.º 1/19 Luxemburgo, 10 de enero de 2019 Conclusiones del Abogado General en el asunto C-136/17 G.C. y otros / CNIL https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-01/cp190001es.pdf

ejercicio de poderes públicos conferidos al responsable del tratamiento" (artículo 20, 3 RGPD).

Pero podemos entender que es un derecho viable en el contexto de la *eHealth*. Así por ejemplo, no siempre fue posible en cloud computing[841]; debido a la existencia de los v*endor lock-in"* que imposibilitaban la migración de un servicio a otro debido a la *incompatibilidad de estándares*. Por eso lo aconsejable es prever y actuar en el momento de la selección y homologación del proveedor cloud, sobre todo si son de terceros países donde no se aplica RGPD. Se recomienda introducir en el encargo de tratamiento (o negociar) la elaboración de un procedimiento de transición como estrategia de salida y como plan de continuidad del negocio, bien como anexo o incluido como clausula, además se deberá negociar -en caso de que se pueda- las causas generales y específicas de resolución

vi. *El derecho a la limitación del tratamiento* a solicitud del interesado, no se podrán tratar sus datos, cuando se den las condiciones siguientes: (a) mientras se verifica la exactitud de los datos en casos de impugnación por el interesado; (b) cuando el tratamiento sea ilícito y el interesado se oponga a la supresión; (b) cuando el interesado necesite que el responsable conserve los datos para el ejercicio o defensa de reclamación; (d) mientras se verifican las circunstancias en el derecho de oposición. Durante el tiempo que dure la limitación, el responsable sólo podrá tratar los datos del afectado para, su conservación o para ejercicio y defensa de reclamaciones o para la protección de derechos de otra persona física o jurídica o por razones de interés público importante (artículo 18.2 RGPD).

vii. El *derecho de la tutela jurisdiccional.* El RGPD estipula que todo interesado, sin perjuicio de cualquier otro recurso administrativo o acción judicial, tendrá derecho a presentar una reclamación ante una autoridad de control si considera que el tratamiento de datos personales que le conciernen infringen el RGPD. Un aspecto

[841] Así por ejemplo, según una según la investigación de la *Universidad de Standford,* el proveedor cloud *Salesforce SaaS,* posibilitaba el retorno de los datos en formato CSV (o estándar) y la posibilidad de descargas semanales o de datos de sus correos electrónicos. Pero al parecer, la mayoría de los proveedores, incluso con un pago adicional no parecen aceptar este tipo de compromiso. Ahora bien, ¿cuánto tiempo dispone el cliente para que pueda recuperar sus datos antes de su eliminación? Muchos proveedores eliminan todo inmediatamente o después de 30 días. Otros ofrecen hasta dos meses (de gracia) o incluso antes de su notificación han llegado a notificar al cliente de la operación. Lo que es claro es que el periodo necesario para migrar aplicaciones de usuario dependerá de las circunstancias. Lo que se recomienda en el periodo contractual es la inclusión de clausulas donde se incluyan duplicados y copias de seguridad. Vid. Kuan Hon, W., Millard, C. Walden, I. (2012). Negotiating cloud contracts: Looking at clouds from both sides now. *Standford Technology Law Review.* Vol. 16. Number 1. Recuperado de http://stlr.stanford.edu/pdf/cloudcontracts.pdf

novedoso que introduce la nueva LOPD es la intervención del Delegado de Protección de Datos en casos de reclamaciones ante la AEPD, al habilitar la posibilidad de que el afectado se dirija con *carácter previo* a la presentación de la reclamación ante la AEPD al DPO, que tendrá un plazo máximo de 2 meses para adoptar la decisión. Las resoluciones de la AEPD agotan la vía administrativa, por lo que pueden ser objeto de recurso de reposición, ante la propia AEPD, y ante la jurisdicción de la Sala de lo Contencioso Administrativo de la Audiencia Nacional.

1.2.7. Nuevos conceptos de datos de salud

El art. 4.15) Reglamento define los datos de salud como *datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud*. Como señala Álvarez Rigaudias (2016, 173)[842], "se trata de una información más amplia que la prevista en el art. 5.1.g del Reglamento de desarrollo de la antigua LOPD que los define como "las informaciones concernientes a la salud pasada, presente y futura o mental de un individuo. En particular se consideran datos relacionados con la salud de las personas los referidos a un porcentaje de discapacidad y a su información genética".

La ampliación conceptual era necesaria esa y prueba de ello fue la sentencia (señalada por la autora), Linqvist del Tribunal de Justicia de la Unión Europea de 6 de noviembre de 2003 (Asunto C-101/01)[843] la cual establece; "…es preciso dar una interpretación amplia a la expresión *datos relativos de salud* (…) de modo que comprenda la información relativa a todos los aspectos, tanto físicos como psíquicos, de la salud de una persona".

En concreto, el considerando 35, señala que "entre los *datos personales relativos a la salud* se deben incluir:

> *"todos los datos relativos al estado de salud* del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro.
>
> Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la

[842] Alavarez Rigaudias, C. (2016) . Tratamiento de datos de salud. En *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad.* Págs 171-185. Dtor. J.L. Piñar. Madrid: Editorial Reus.

[843] Cfr. Sentencia del Tribunal de Justicia, de 6 de noviembre de 2003. Asunto C-101/01. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62001CJ0101&from=EN

> Directiva 2011/24/UE del Parlamento Europeo y del Consejo (1); *todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas*, y cualquier información relativa, a título de ejemplo, a *una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado*, independientemente de su fuente, por ejemplo un *médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro".*

Como señala ALVAREZ, "la definición del Reglamento no sólo se refiere a datos directamente relacionados con la salud de una persona (física o mental) sino que también incluye información sobre el "estado de salud" tal y como hemos visto en el considerando citado.

Detengámonos en los *datos genéticos*. También se incorpora un concepto para éstos (en el apartado 13, del art. 4) regulando el tratamiento de este tipo de datos con algunos cambios en relación con la Directiva[844]:

> "Son datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona";

En concreto, el considerando 34 establece que debe entenderse por *datos genéticos*;

> "a los datos personales relacionados con características genéticas, heredadas o adquiridas, de una persona física, provenientes del análisis de una muestra biológica de la persona física en cuestión, en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente"

Dadas las particularidades y "debido a los condicionamientos ideológicos, religiosos, filosóficos, culturales, jurídicos y al sometimiento de la evolución y desarrollo continuo, se contempla la posibilidad de que los Estados miembros de la Unión, puedan mantener o introducir de manera específica *condiciones adicionales* mediante la formulación de las correspondientes limitaciones, con relación al tratamiento de los *datos genéticos, los datos biométricos, o los datos relativos a la salud en general*. Por lo tanto, las facultades normativas que se conceden a los Estados van encaminadas en tres direcciones bien distintas; el mantenimiento de las condiciones establecidas en el

[65] PÉREZ GÓMEZ, J.M. « La protección de los datos de salud », en A. RALLO LOMBARTE, R. GARCÍA MAHAMUT (coords.), *Hacia un nuevo derecho europeo de protección de datos*, Tirant lo Blanch, Valencia, 2015, pp. 629 y ss.

RGPD, la posibilidad de establecer condiciones adicionales, y finalmente, la introducción de limitaciones a tal normativa" (PUYOL, 2016,148).

En definitiva, hemos pasado de una norma como la Directiva 95/46/CE, en la que apenas se contenían referencias a los datos de salud (más allá de las reglas genéricas establecidas para el tratamiento de categorías especiales de datos, art. 8) a otra como el RGPD.[845]

1.2.8. Transferencias internacionales

"La rápida *evolución tecnológica y la globalización* han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. (…) La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un *elevado nivel de protección* de los datos personales" (Considerando 6 RGPD). En definitiva, partimos de la premisa de que se podrán hacer transferencias internacionales solo si se cumple el Reglamento europeo *(Considerando 101 RGPD).*

3.2.8.1.De "puerto seguro" al "escudo de privacidad".

Desde finales del año 2015, las transferencias internacionales de datos de carácter personal han tenido una relevancia pública tras las revelaciones incluidas en el denominado caso *Snowden* y, sobre todo, con la sentencia del Tribunal de Justicia de la Unión Europea, que *invalidó* la *Decisión de Puerto Seguro* de la Comisión Europea que consideraba que las entidades de Estados Unidos adheridas a dicho sistema adoptado por la Comisión europea en el año 2000 *proporcionaban un nivel adecuado* de protección, y que dio lugar a que muchos responsables de ficheros adquirieran conciencia de que estaban realizando transferencias internacionales con motivo de la

[845] El cual incorpora definiciones y referencias múltiples al tratamiento de estos datos y que responde a las necesidades planteadas en los últimos tiempos de utilización de la información sanitaria en ámbitos como la salud pública, la gestión de los servicios sanitarios y de protección social y la investigación científica, creemos que apostando claramente por un mayor aprovechamiento de la información y la utilización de los datos personales. Siendo éste el camino trazado por el Reglamento, la clave estará en cómo se apliquen las garantías de los derechos de las personas afectadas a los que también se hace referencia en estas normas. Por lo que habrá que hacer especial hincapié en esas medidas de protección de los derechos de los interesados que se van a implementar fundamentalmente por las legislaciones nacionales, dado el amplio margen de actuación que tienen los Estados miembros en esta materia.

contratación de determinados servicios, fundamentalmente de *cloud computing*. El Puerto Seguro fue sustituido por el denominado acuerdo del *Escudo de Privacidad (Privacy Shield*) como sistema de garantías para poder transmitir datos a aquellas entidades establecidas en los Estados Unidos de América que hayan optado por adherirse al sistema de garantías para las transferencias internacionales incluidas en dicho marco. Con él llegaron los cambios ya que *sólo* se podrán transmitir datos a aquellos países, territorios, sectores u organismos internacionales respecto de los que la Comisión Europea haya considerado que; disponen de un nivel adecuado de protección[846] o, se aporten garantías suficientes o, se den algunas de las circunstancias previstas como excepciones, y siempre y cuando se observen los demás requisitos del mencionado RGPD.

3.2.8.3.Responsables y encargados "exportadores".

El RGPD establece que el exportador de datos puede ser tanto un responsable como un encargado del tratamiento. Lo que da lugar a que los prestadores de servicio establecidos en terceros países se encuentren en mejor situación a la hora de subcontratar en esos u otros terceros países que los prestadores de servicios establecidos en la UE. Esta situación fue abordada por la AEPD mediante la adopción de las cláusulas contractuales. Así mismo, se amplía el abanico de instrumentos como los códigos de conducta y los mecanismos de certificación y las Normas Corporativas Vinculantes de las que hablaremos más adelante.

3.2.8.4.Ausencia de adecuación en las transferencias internacionales.

En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el responsable o el encargado del tratamiento *deben tomar medidas para compensar la falta de protección de datos* en un tercer país mediante garantías adecuadas para el interesado. Se deben poner a disposición de los interesados sus *derechos exigibles y de acciones legales efectivas*, incluyendo el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización, en la

[846] Según la AEPD, hasta la fecha la *Comisión Europea* ha considerado países que ofrecen un *nivel adecuado* de protección a los siguientes países y territorios: Suiza, Argentina, Guernsey, Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda; Canadá (sólo cuando a la entidad destinataria le sea de aplicación la "Personal Information and Electronic Documents Act") y Estados Unidos (sólo cuando la entidad destinataria de los datos este certificada en el esquema del Escudo de Privacidad). Para más info: https://www.aepd.es/reglamento/cumplimiento/transferencias-internacionales.html

Unión o en un tercer país. En particular, deben referirse al cumplimiento de los *principios generales* relativos al tratamiento de los datos personales y los principios de la protección de datos desde el diseño y por defecto.

3.2.8.5.Principal novedad: autorización y notificación previa.

Donde más evidente son las novedades que introduce el RGPD es en el régimen de *autorización y notificación previa* de las transferencias internacionales, que quedan reducidas a muy pocos supuestos. Antes se obligaba a los exportadores de datos a solicitar una autorización previa para poder transferir datos a importadores establecidos en países que no contaban con un nivel adecuado de protección, siempre que aporten las garantías suficientes, y a notificar las transferencias cuando se dirigen a países que sí disponen de dicho nivel adecuado. Ahora con carácter general, las transferencias se pueden llevar a cabo sin necesidad de autorización previa, salvo que las garantías se aporten a través de: un *contrato entre el responsable o el encargado del tratamiento*, encargado o destinatario de los datos personales en el tercer país u organización internacional, o de un *acuerdo administrativo* entre autoridades públicas, supuestos en los que será preciso que exista la autorización de la autoridad de control, tal y como señala el artículo 46.3 del RGPD.

3.2.8.6.Garantías adecuadas sin necesidad de autorización expresa.

En el artículo 46 del Reglamento se relacionan las garantías adecuadas que podrán ser aportadas *sin que se requiera ninguna autorización expresa* de una autoridad de control; un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos; normas corporativas vinculantes; cláusulas tipo de protección de datos adoptadas por la Comisión; cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión; un código de conducta; un mecanismo de certificación.

Aunque existen excepciones de autorización para situaciones específicas:

i. Se debe establecer la posibilidad de realizar transferencias en determinadas circunstancias, de mediar el *consentimiento explícito* del interesado:
ii. Si la transferencia es ocasional y necesaria en relación con un contrato o una reclamación, independientemente de tratarse de un procedimiento judicial o un procedimiento administrativo o extrajudicial, incluidos los procedimientos ante organismos reguladores.

iii. Si lo requieran razones importantes de *interés público* establecidas por el Derecho de la Unión o de los Estados miembros.

iv. Si la transferencia se hace a partir de un registro establecido por ley y se destine a consulta por el público o por personas que tengan un interés legítimo (Considerando 111). Por ejemplo, piénsese en el caso de contactos destinados a localizar enfermedades contagiosas.

v. La transferencia de datos personales también debe considerarse lícita en caso de que sea necesaria para proteger un interés esencial para los *intereses vitales del interesado* o de otra persona, incluida la integridad física o la vida, si el interesado no está en condiciones de dar su consentimiento.

3.2.9. Las normas corporativas vinculantes o "Binding Corporate Rules"

El apartado 20 del artículo 4 del RGPD las define como:

> "Las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro[847] para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, *dentro de un grupo empresarial* o una unión de empresas dedicadas a una *actividad económica conjunta*".

Señalemos a continuación algunas conclusiones interesantes:

En primer lugar, las normas corporativas vinculantes consisten en *políticas internas* de un grupo de empresas que se convierten en vinculantes traduciéndose en un marco de actuación aplicable a las operaciones internacionales de tratamiento de datos. Suponen un instrumento de "homogeneización" para fomentar la adopción de estándares de privacidad a una pluralidad de destinos que no tienen una misma normativa aplicable o que cuentan con estándares diferentes[848]. Es entendible que los grupos empresariales pueden estar formados por organizaciones asentadas en zonas geográficas dispares con diferente cultura de privacidad. Mientras que no se instauren unos estándares de seguridad a nivel internacional este instrumento se presenta como el más adecuado. Hay que tener en cuenta, además, que éstas normas se deben amoldar a la propia naturaleza del negocio (pensemos en la industria farmacéutica). En todo caso, gracias a este instrumento se desarrollará una cultura de privacidad

[847] La AEPD y las autoridades autonómicas de protección de datos podrán aprobar normas corporativas vinculantes de acuerdo con lo previsto en el Reglamento europeo. (Art. 41.2 LOPDGDD)

[848] Cfr. https://www.elmundo.es/economia/empresas/2019/01/22/5c47118bfc6c83384a8b45e9.html

En segundo lugar, lo que es más importante, están reconocidas por el RGPD como "instrumento de evidencia" de *una protección adecuada* para las transferencias de datos personales fuera de la UE, y por las autoridades de protección de datos de la UE como una *vía de cumplimiento de las responsabilidades* marcadas por el RGPD.

En tercer lugar, estos instrumentos tienen una gran ventaja para las organizaciones; la eliminación de las "clausulas contractuales tipo" entre los componentes del grupo empresarial, ya que las normas corporativas vinculantes permiten la libre circulación de datos basados únicamente en ese instrumento (dentro y fuera del grupo). No sólo eso, las normas corporativas vinculantes se han visto como medidas simplificadoras de los procesos burocráticos de autorización de las transferencias internacionales de datos en el contexto de globalización e interconexión de organizaciones del sector privado.

En cuarto lugar, tengamos en cuenta el contenido mínimo de las normas corporativas vinculantes será:

1. la *estructura y los datos de contacto* del grupo empresarial y de cada uno de sus miembros;
2. las *transferencias* (incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de interesados afectados y el nombre del tercer o los terceros países en cuestión)
3. su *carácter jurídicamente vinculante*, tanto a nivel interno como externo;
4. la aplicación de los *principios* generales en materia de protección de datos
5. los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos
6. la *aceptació*n por parte del responsable o del encargado del tratamiento establecidos en el territorio de un Estado miembro de la *responsabilidad* por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión.
7. la *forma* en que se facilita a los interesados *la información* sobre las normas corporativas vinculantes (aptdos. d), e) y f) y art. 13 y 14 RGPD)
8. las *funciones de todo delegado de protección de datos* designado de conformidad con el artículo 37, *o de cualquier otra persona o entidad encargada* de la supervisión del cumplimiento de las normas corporativas vinculantes.
9. los *procedimientos de reclamación*;
10. los mecanismos establecidos dentro del grupo empresarial para garantizar la verificación del cumplimiento de éstas. Por ejemplo, auditorías y métodos para garantizar acciones correctivas.

11. el *mecanismo de cooperación con la autoridad de control* para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial.
12. los *mecanismos para informar a la autoridad de control* competente de cualquier requisito jurídico de aplicación en un país tercero a un miembro del grupo empresarial que probablemente tengan un efecto adverso sobre las garantías establecidas en éstas.
13. la *formación en protección de datos* pertinente para el personal que tenga acceso permanente o habitual a datos personales.

A modo de conclusión, evidenciamos que el efecto de la regulación de las normas vinculantes corporativas surge como respuesta del legislador en la *búsqueda de estrategias garantistas* en beneficio de los derechos y libertades de las personas. Por otro lado, se debería reconoce por parte de los stakeholders el *esfuerzo de los solicitantes* de las misma ya que se trata de un acto voluntario, de hecho, como hemos dicho supondrá un "instrumento de evidencia" de cumplimiento normativo frente al resto. Ahora bien, si analizamos el grado de acogida de este instrumento posiblemente nos enfrentemos con la dura realidad. Me parece importante destacar algo respecto al *objeto y alcance* de este instrumento regulatorio. Nos encontramos en un contexto globalizado donde las operaciones mercantiles se realizan entre diferentes puntos del mundo y donde la circulación de datos es inevitable.; ¿por qué limitar su uso a grupos o uniones empresariales?¿porque no extenderlo a organizaciones que tienen entre ellas relación mercantil y realizan operaciones comerciales? ¿Por qué no se podría aprovechar este instrumento jurídico vinculante como *"smart contract"* implementado en un sistema *DLT/Blockchain de salud* donde compañías farmacéuticas y empresas tecnológicas y aseguradoras tuvieran las mismas normas vinculantes con los requisitos citados en el punto anterior en materia de protección de datos?[849]

[849] Desde mi humilde punto de vista se ha desperdiciado la oportunidad de aprovechar al máximo esta figura y extenderla su aplicabilidad a un mayor número de participantes. Quizás ese desperdicio ha venido generado por las excesivas y optimistas perspectivas volcadas en los estándares internacionales. Si bien es cierto, a priori, podría resultar demasiada carga de supervisión por parte de las autoridades de control se podría preveer otras medidas complementarias y de apoyo que lo sufragaran.

2. EL NUEVO MARCO NORMATIVO ESPAÑOL DE PROTECCIÓN DE DATOS

2.1. Antecedentes de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD)

Tal y como señala el legislador en el Preámbulo I de la LOPDGDD ; "a nivel legislativo, la concreción y desarrollo del *derecho fundamental*[850] *de protección de las personas físicas en relación con el tratamiento de datos personales* tuvo lugar en sus orígenes mediante la aprobación de la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales, conocida como LORTAD. La Ley Orgánica 5/1992 fue reemplazada por la Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales, a fin de trasponer a nuestro derecho a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta ley orgánica supuso un segundo hito en la evolución de la regulación del derecho fundamental a la protección de datos en España y se complementó con una cada vez más abundante jurisprudencia procedente de los órganos de la jurisdicción contencioso-administrativa".

Es finalmente en el 23 de junio de 2017, cuando el Consejo de Ministros recibía el informe del Ministerio de Justicia al Anteproyecto de la Ley Orgánica de Protección de Datos de Carácter Personal. Se derogó la antigua Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), y se aprobó la nueva

---

[850] En dicho Preámbulo I, el legislador nacional destaca algo de especial relevante (y que hemos mencionado en el capitulo 6); "El TC señaló en su Sentencia 94/1998, de 4 de mayo, que nos encontramos ante un derecho fundamental a la protección de datos por el que se *garantiza a la persona el control sobre sus datos*, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una *facultad del ciudadano para oponerse* a que determinados datos personales sean usados para *fines distintos* a aquel que justificó su obtención. Por su parte, en la Sentencia 292/2000, de 30 de noviembre, lo considera como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso". En otro orden de cosas, decir que no deja de ser llamativo como "los constituyentes de 1978 ya intuyeron el enorme impacto que los avances tecnológicos provocarían en nuestra sociedad y, en particular, en el disfrute de los derechos fundamentales" (Preámbulo IV LOPDGDDD).

la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), completando así el ordenamiento jurídico vigente en materia de protección de datos y entrando en vigor el 7 de diciembre de 2018. Con la nueva LOPDGDD se pretende adaptar la regulación actual al Reglamento europeo 2016/679 (RGPD) que entró en vigor el pasado 25 de mayo.
Cuando entró en vigor la LOPDGDD quedaron derogados la LOPD, el Real Decreto-ley 5/2018, de 27 de julio, así como todas aquellas disposiciones de igual o inferior rango que contradigan, se opongan, o resulten incompatibles con lo dispuesto en el RGPD y en la propia LOPDGDD.

2.2. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales(LOPDGDD)

2.2.1. El objeto y ámbito de aplicación

El considerando 8 del RGPD permite que los EEMM incorporen a su derecho nacional elementos del mismo, en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sea comprensibles para sus destinatario. Existen unos *amplios márgenes de maniobra* conferidos a los Estados miembros (considerando 10) en ocasiones donde hay vacíos regulatorios en beneficio del "Derecho de los Estados" en las siguientes materias: el procesamiento de datos por *obligación legal; e*l tratamiento realizado en misiones de *interés público; e*l tratamiento que llevan a cabo los poderes públicos de un determinado Estado; las que el RGPD denomina "situaciones específicas" de tratamiento de los que el RGPD "se desentiende":

i. Libertad de expresión e información (art. 85 RGPD)
ii. Acceso público a los documentos oficiales (art. 86 RGPD)
iii. Número nacional de identificación (art. 87 RGPD)
iv. Ámbito laboral (art. 88 RGPD)
v. Fines de archivo en interés público, *fines de investigación científica o histórica o fines estadísticos (art. 89 RGPD)*
vi. Y protección de datos de iglesias y asociaciones religiosas (art. 91 RGPD).

De hecho, también, en el Preámbulo (III) de la nueva LOPDGDD, se hace referencia a lo anterior, señalando que "el RGPD contiene un buen número de habilitaciones, cuando no imposiciones, a los Estados miembros, a fin de regular determinadas materias, permitiendo incluso en su considerando 8, y a diferencia de lo

que constituye principio general del Derecho de la Unión Europea que, cuando sus normas deban ser especificadas, interpretadas o, excepcionalmente, restringidas por el Derecho de los Estados miembros, estos tengan la posibilidad de *incorporar al derecho nacional previsiones contenidas específicamente en el reglamento*, en la medida en que sea necesario *por razones de coherencia y comprensión*." Esta es la razón por la que aún sin ser necesario incorporar esa normativa en nuestra propia legislación, el legislador nacional lo ha considerado así para obtener una mayor comprensión, seguridad jurídica y transparencia pública (si se puede decir así).

Señala el legislador que "los Reglamentos, pese a su característica de aplicabilidad directa, en la práctica pueden exigir otras normas internas complementarias para hacer plenamente efectiva su aplicación. En este sentido, más que de incorporación cabría hablar de «desarrollo» o complemento del Derecho de la Unión Europea".

Podríamos decir que el *objeto* de la ley orgánica es doble: por un lado, se pretende lograr la *adaptación* del ordenamiento jurídico español al Reglamento y a su vez, *establecer que el derecho fundamental* de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución[851], se ejercerá con arreglo a lo establecido en el Reglamento y en esta ley orgánica.

Pero además, es también objeto de la Ley garantizar los *derechos digitales* de la ciudadanía, al amparo de lo dispuesto en el artículo 18.4 de la Constitución. Destaca la novedosa regulación de los datos referidos a las *personas fallecidas*, pues, tras excluir del ámbito de aplicación de la ley su tratamiento, se permite que las personas vinculadas al fallecido por razones familiares o de hecho o sus herederos puedan solicitar el acceso a los mismos, así como su rectificación o supresión, en su caso con sujeción a las instrucciones del fallecido. Además, las comunidades autónomas ostentan competencias de desarrollo normativo y ejecución del derecho fundamental a la protección de datos

[851] Este artículo establece que *"la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".* Ya el legislador hace más de tres décadas vaticinaba el cambio de paradigma tecnológico que estaba por llegar y se refería con ese precepto a la llamada "libertad informática" como el *derecho a controlar* el uso de los mismos datos insertos en un programa informático (habeas data) comprendiendo entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, FJ 5, 94/1998, FJ 4).

personales en su ámbito de actividad y a las autoridades autonómicas de protección de datos que se creen les corresponde contribuir a garantizar este derecho fundamental de la ciudadanía. En todo caso, la razón última de esta nueva Ley Orgánica es procurar seguridad jurídica.

Con respecto al ámbito de aplicación, se establece que se aplicará lo dispuesto en los Título I a IX y en los artículos 89 a 94, a cualquier tratamiento de datos personales contenidos o destinados a ser incluidos en un fichero, ya sea total o parcialmente automatizado así como no automatizado. Exceptuándose en su aplicación en el caso de: (i) "tratamientos excluidos del ámbito de aplicación del RGPD; (ii) tratamientos de datos de personas fallecidas, salvo lo indicado en el artículo 3; y (iii) tratamientos sometidos a normativa sobre protección en materias clasificadas".

2.2.2. Novedades

Se establece en el Preámbulo V de la Ley Orgánica que "a efectos del Reglamento no serán imputables al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos obtenidos directamente del afectado, cuando hubiera recibido los datos de otro responsable en virtud del ejercicio por el afectado del *derecho a la portabilidad*, o cuando el responsable los obtuviese del mediador o intermediario cuando las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establezcan la posibilidad de intervención de un intermediario o mediador o cuando los datos hubiesen sido obtenidos de un registro público".

A modo de resumen, el legislador continua señalando que "también se recoge expresamente el *deber de confidencialidad*, el tratamiento de datos amparado por la ley, las categorías especiales de datos y el tratamiento de datos de naturaleza penal, se alude específicamente al consentimiento, que ha de proceder de una declaración o de una clara acción afirmativa del afectado, excluyendo lo que se conocía como "consentimiento tácito", se indica que el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que se otorga para todas ellas, y se mantiene en catorce años la edad a partir de la cual el menor puede prestar su consentimiento".

2.2.3. Disposiciones adicionales y finales en materia de salud de la LOPDGDD

En primer lugar, corresponde mencionar el apartado 1 de la *disposición adicional decimoséptima referente a los tratamientos de datos de salud y genéticos* por la que se señala que se encuentran amparados los *apartados g), h), i) y j) del artículo 9.2 del Reglamento* que estén regulados en las siguientes leyes y sus disposiciones de desarrollo:

> *a) La Ley 14/1986, de 25 de abril, General de Sanidad*.
>
> b) La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.
>
> *c) La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.*
>
> *d) La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.*
>
> e) La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.
>
> *f) La Ley 14/2007, de 3 de julio, de Investigación biomédica.*
>
> *g) La Ley 33/2011, de 4 de octubre, General de Salud Pública.*
>
> *h) La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.*
>
> *i) El texto refundido de la Ley de garantías y uso racional de 105 medicamentos y productos sanitarios, aprobado por Real Decreto Legislativo 1/2015, de 24 de julio.*
>
> j) El texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013 de 29 de noviembre.

En segundo lugar, corresponde mencionar la *disposición final quinta* que incluye la *Modificación de la Ley 14/1986, de 25 de abril, General de Sanidad* y se añade un nuevo "capítulo II" denominado "Tratamiento de datos de la investigación en salud. Artículo 105 bis.":

> "El tratamiento de datos personales en la investigación en salud se regirá por lo dispuesto en la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales."

Me parece importante destacar dos aspectos; (i) el papel importante de la investigación sanitaria y la necesidad de la actualización de su regulación treinta años después de la creación de la LGS; (ii) el nacimiento de los derechos digitales, también en el área de salud digital y su implicación y su "trasposición" al resto de leyes nacionales.

En tercer lugar, corresponde también señalar, la *disposición final novena* que incluye la *Modificación de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica* por la que se modifica el apartado 3 del artículo 16 de la Ley

41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica[852].

Es decir, por cuanto nos interesa destacamos de esta disposición que; (i) para acceder a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se requiere conservar los datos de identificación personal del paciente, separados de los de carácter *clínico asistencial* (consiguiendo e*l anonimato)*, salvo que el paciente indique lo contrario; (ii) no obstante, si hablamos de investigación, habrá que acudir a las excepciones que se refiere el legislador en la disposición adicional séptima, aptdo. 2 (del que hablaremos más adelante); (iii) cuando sea necesario el tratamiento por motivos de prevención de peligro grave para la salud, las Administraciones Sanitarias podrán acceder a los datos identificativos con motivación previa y secreto profesional por parte del profesional sanitario.

Disposición adicional decimoséptima	Disposición final quinta	Disposición final novena
9.2. g, h, i y j.a la LGS, LPRL, Ley de autonomía del paciente, Ley Cohesión y calidad, Ley profesiones sanitarias, LIB, LGSP, Ley entidades aseguradoras, Ley medicamentos y productos sanitarios, Ley personas con discapacidad.	Modifica LGS y añade Tratamiento de datos de la investigación en salud. Artículo 105 bis.	Modifica Ley autonomía del paciente: Acceso historial médico; anonimato

[852] Que pasa a tener el siguiente tenor: "El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico asistencial, de manera que, como regla general, *quede asegurado el anonimato*, salvo que el propio paciente haya dado su consentimiento para no separarlos. *Se exceptúan los supuestos de investigación* previstos en el apartado 2 de la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.(..) Cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, de 4 de octubre, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por *razones epidemiológicas o de protección de la salud pública*[852]. El acceso habrá de realizarse, en todo caso, *por un profesional sanitario sujeto al secreto profesional* o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos."

Tabla 48. Resumen breve de las Disposiciones LOPDGDD que afectan a la I. del Cuidado de la Salud.

2.2.4. Legitimación.

Respecto al *consentimiento* como base legitimadora (art. 6 LOPDGDD), el legislador nacional resalta la importancia de que el consentimiento cumpla ciertos requisitos de acuerdo con el art. 4.11 RGPD, asumiendo que este es toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa. Además también será preciso en caso de pluralidad de consentimientos otorgar el consentimiento para todas ellas. Y clarifica que "no podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual" (art. 6.3 LOPDGDD).

En el preámbulo V, también, el legislador señala que algo que nos interesa bastante: "*el RGPD no afecta a habilitaciones legales, que siguen plenamente vigentes, permitiendo incluso llevar a cabo una interpretación extensiva de las mismas, como sucede, en particular, en cuanto al alcance del consentimiento del afectado o el uso de sus datos sin consentimiento en el ámbito de la investigación biomédica".* Además, "a tal efecto, como hemos visto, el apartado 2 de la Disposición adicional séptima introduce una serie de previsiones encaminadas a garantizar el adecuado desarrollo de la investigación en materia de salud, y en particular la biomédica, ponderando los indudables beneficios que la misma aporta a la sociedad con las debidas garantías del derecho fundamental a la protección de datos".

Respecto a la *obligación legal exigible al responsable* (aseguradoras, investigadores, hospitales, tecnológicas, empresas farmacéuticas) como base legitimadora, el legislador señala que será de acuerdo con el art. 6.1.c) del Reglamento, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Además dicha norma podrá igualmente imponer condiciones especiales al tratamiento, como medidas adicionales de seguridad u otras (art. 8.1.LOPDGDD).

Y por último, el legislador nacional establece que "el tratamiento de datos personales solo podrá considerarse fundado en el *cumplimiento de una misión realizada en interés público o en el ejercicio de poderes público*s conferidos al responsable, en los

términos previstos en el artículo 6.1 e) del Reglamento, cuando derive de una competencia atribuida por una norma con rango de ley" (Art. 8.2.LOPDGDD).

2.2.5. Derechos de los titulares de datos personales de salud

La ley orgánica contempla los derechos de acceso, rectificación, supresión, oposición, derecho a la limitación del tratamiento y derecho a la portabilidad explicados anteriormente.

También la L.O. adapta al Derecho español el principio de transparencia y el *deber de información (Art. 13)* y recoge la denominada «*información por capas*»: "en un primer nivel, presentar una información básica (identificación del responsable, finalidad del tratamiento, ejercicio de derechos, origen de los datos, realización de perfiles), de forma resumida, en el mismo momento y medio en que se recojan los datos; y en un segundo nivel, la información adicional, presentando de forma detallada el resto de informaciones (podría incluirse la política de privacidad)".

Epígrafe	**Información básica (1ª capa)**	**Información adicional (2ª capa)**
Responsable del tratamiento	Identidad del responsable del tratamiento	-Datos de contacto del responsable - Datos del contacto DPO
Finalidad del tratamiento	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles	-Descripción ampliada de los fines del tratamiento Plazos o criterios de conservación de los datos -Decisiones automatizadas, perfiles y lógica aplicada
Legitimación del tratamiento	Base jurídica del tratamiento	- Detalle de la base jurídica en los casos de obligación legal, interés público o interés legítimo. - Obligación o no de facilitar datos y consecuencias de no hacerlo
Destinatarios (de cesiones o transferencias)	- Previsión o no de cesiones -Previsión de transferencias, o no, a terceros países.	-Destinatarios o categorías de destinatarios -Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables
Derechos (de las personas interesadas)	Referencia al ejercicio de los derechos	- Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento -Derecho a retirar su consentimiento
Procedencia de los datos	Fuente de los datos cuando no proceden del interesado	-Información detallada del origen de los datos incluso si proceden de fuentes de acceso público

		-Categorías de datos que se traten

Tabla 49. Deber de información de doble capa. .Fuente: Contenido AEPD[853]

En todo caso, la APDCAT señala que "el RGPD no establece la obligación de informar respecto a la contratación de un encargado del tratamiento. Pese a esto, en determinadas circunstancias (atendiendo, por ejemplo, a la naturaleza del tratamiento o de los datos tratados, o por otras circunstancias concurrentes) puede ser aconsejable dar esta información para una mayor transparencia en el tratamiento de los datos personales".

Resultó de interés destacar la proposición formulada en 2013 por la Comisión LIBE del Parlamento Europeo en sus enmiendas a la propuesta del RGPD:

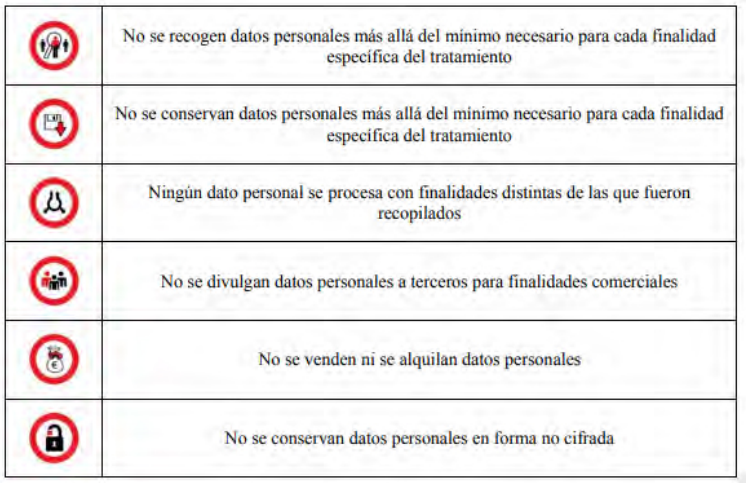


Imagen 69. Ejemplo de información iconográfica. Fuente Comisión LIBE[854].

¿Por qué no utilizar esta iconografía para informar de forma clara a los usuarios de cuestiones como estas en aplicaciones con tecnologías implicadas como IA o Blockchain?

[853] AEPD. Protección de datos. Guía para el ciudadano. Recuperado de https://www.aepd.es/media/guias/guia-ciudadano.pdf

[854] Vid. Parlamento Europeo (21 de noviembre de 2013). Informe sobre sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)). Recuperado de http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//ES

Por otro lado, aparecen también los *"derechos digitales"* bajo el Título X "garantía de los derechos digitales" contemplados del artículo 79 al 99 de la LOPDGDD**.** En concreto, se establece que "los derechos y libertades consagrados en la Constitución y en los Tratados y Convenios Internacionales en que España sea parte son plenamente aplicables en internet. Los prestadores de servicios de la sociedad de la información y los proveedores de servicios de Internet contribuirán a garantizar su aplicación". Tal y como establece el legislador nacional en la LOPDGDD en la exposición de motivos, "corresponde a los poderes públicos impulsar políticas que hagan efectivos los derechos de la ciudadanía en Internet promoviendo la igualdad de los ciudadanos y de los grupos en los que se integran para hacer posible el pleno ejercicio de los derechos fundamentales en la realidad digital".[855]

En concreto se tratarías de las siguientes (del artículo 79 al 99):

- Derecho a la neutralidad de Internet.
- Derecho de acceso universal a Internet.
- Derecho a la seguridad digital.
- Derecho a la educación digital.
- Protección de los menores en Internet.
- Derecho de rectificación en Internet.
- Derecho a la actualización de informaciones en medios de comunicación digitales.
- Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.
- Derecho a la desconexión digital en el ámbito laboral.
- Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.
- Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.
- Derechos digitales en la negociación colectiva.
- Protección de datos de los menores en Internet.
- Derecho al olvido en búsquedas de Internet.
- Derecho al olvido en servicios de redes sociales y servicios equivalentes.
- Derecho de portabilidad en servicios de redes sociales y servicios equivalentes.

[855] Además, el legislador establece que "los constituyentes de 1978 ya intuyeron el enorme impacto que los avances tecnológicos provocarían en nuestra sociedad y, en particular, en el disfrute de los derechos fundamentales Una deseable futura reforma de la Constitución debería incluir entre sus prioridades la actualización de la Constitución a la era digital y, específicamente, elevar a rango constitucional una nueva generación de derechos digitales. Pero, en tanto no se acometa este reto, el legislador debe abordar el reconocimiento de un *sistema de garantía de los derechos digitales* que, inequívocamente, encuentra su anclaje en el mandato impuesto por el apartado cuarto del artículo 18 de la Constitución Española y que, en algunos casos, ya han sido perfilados por la jurisprudencia ordinaria, constitucional y europea".

- Derecho al testamento digital.
- Políticas de impulso de los derechos digitales.

A destacar desde mi humilde punto de vista respecto lo que nos concierne los siguientes:

i. Derecho a la seguridad digital. (*Art. 82 LOPDGDD)*

Los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet y los proveedores de servicios de Internet informarán a los usuarios de sus derechos.

*ii. Derecho de rectificación en Internet. (*Art. 85.LOPDGDD)

Se establece que los responsables de redes sociales, plataformas digitales y servicios de la sociedad de la información equivalentes deberán adoptar y ejecutar protocolos efectivos para garantizar el ejercicio del derecho de rectificación, en particular en relación con los contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en Internet y el derecho a comunicar o recibir libremente información veraz.

*iii. Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral. (*Art. 87. LOPDGDD)

Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente.

iv. Derecho al olvido en servicios de redes sociales y servicios equivalentes. (Art.94 LOPDGDD)

Se reconoce el derecho de las personas a que se supriman datos personales publicados por servicios de RRSS y servicios de la sociedad de la información, también los facilitados por terceros cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información. Se exceptúan de lo dispuesto en este apartado los datos que hubiesen sido facilitados por personas físicas en el ejercicio de actividades personales o domésticas.

v. Derecho al testamento digital. (Art.96.LOPDGDD)

Se regula el acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas. Se señala que "las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos podrán dirigirse a los prestadores de servicios de la sociedad de la información al objeto de acceder a dichos contenidos e impartirles las instrucciones que estimen oportunas sobre su utilización, destino o supresión. Como excepción, las personas mencionadas no

podrán acceder a los contenidos del causante, ni solicitar su modificación o eliminación, *cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley*…".

2.2.6. Principio de responsabilidad activa.

El legislador nacional quiere destacar el cambio que se produce en la relación de responsable-encargado de tratamiento señalando que "es preciso tener en cuenta que la mayor novedad que presenta el Reglamento es la evolución de un modelo basado, fundamentalmente, en el *control del cumplimiento* a otro que descansa en el *principio de responsabilidad activa,* lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de dicha valoración, adoptar las medidas que procedan".
Por otro lado, es importante destacar que los contratos de encargo de tratamiento de datos personales entre las organizaciones (como responsables) y terceros (como encargados de tratamiento) suscritos antes del 25 de mayo de 2018 mantendrán su vigencia como máximo hasta el 25 de mayo de 2022.

2.2.7. El DPO.

En el preámbulo V, se señala que "la figura del *delegado de protección de datos* adquiere una destacada importancia en el Reglamento y así lo recoge la ley orgánica, que parte del principio de que puede tener un carácter obligatorio o voluntario, estar o no integrado en la organización del responsable o encargado y ser tanto una persona física como una persona jurídica. La designación del delegado de protección de datos ha de comunicarse a la autoridad de protección de datos competente. La Agencia Española de Protección de Datos mantendrá una relación pública y actualizada de los delegados de protección de datos, accesible por cualquier persona. Los conocimientos en la materia se podrán acreditar mediante esquemas de certificación. Asimismo, no podrá ser removido, salvo en los supuestos de dolo o negligencia grave. Es de destacar que el delegado de protección de datos permite configurar un medio para la resolución amistosa de reclamaciones, pues el interesado podrá reproducir ante él la reclamación que no sea atendida por el responsable o encargado del tratamiento".

El responsable del tratamiento de datos deberá hacer conocer la dirección del correo electrónico del DPO o la dirección postal para que los interesados puedan aclarar dudas o necesidades en materia de protección de datos.

3. LA NORMATIVA SECTORIAL ESPECÍFICA.

3.1. La Ley 14/1986, de 25 de abril, General de Sanidad.

Se señala que la organización sanitaria **debe permitir garantizar la *protección de la salud* como un *derecho inalienable*** y que debe asegurarse en condiciones de escrupuloso respeto a *la intimidad personal y a la libertad individual* del usuario, garantizando *la confidencialidad* de la información relacionada con los servicios sanitarios que se prestan, y sin ningún tipo de discriminación.

Hay que tener en cuenta, como hemos dicho, y por cuanto nos incumbe, la novedad que incorpora el apartado 3 del artículo 16 de la Ley 41/2002 (disposición novena final LOPDGDD) que establece que "el acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, *de investigación o de docencia*, se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso". Esta disposición, por ejemplo, afectará por cuanto nos interesa en materia de investigación biomédica y *big data*, como veremos.

i. La Ley 16/2003 de 28 de mayo de Cohesión y Calidad del Sistema nacional de salud[856].

Su ámbito de aplicación incluirá entre otras acciones las prestaciones sanitarias sino también con la farmacia, la investigación o la participación de los ciudadanos y profesionales (Art.5). Y coordinará los mecanismos de intercambio electrónico de información clínica y salud individual, para permitir el acceso, tanto al usuario como a los profesionales, con la finalidad de garantizar la calidad de la asistencia y la *confidencialidad* e integridad de la información (Art. 56). En todo caso este artículo en lo relativo al intercambio de información telemática entre organismos, centros y servicios del Sistema Nacional de Salud se deberá adaptar a la Ley Orgánica de

[856] Vid. http://noticias.juridicas.com/base_datos/Admin/l16-2003.html#a1

Protección de datos y Garantía de derechos digitales de 5 de diciembre de 2018 para garantizar la confidencialidad e integridad de la información.

ii. Ley 41/2002, de 14 de noviembre, de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica[857].

Tiene por objeto la regulación de los derechos y obligaciones de los pacientes, usuarios y profesionales, así como de los centros y servicios sanitarios, públicos y privados, en materia de autonomía del paciente y de información y documentación clínica.

En todo caso, y al margen de las legislaciones mencionadas y poniendo la vista en futuros desarrollos normativos donde pudieran verse comprometidos datos personales y la privacidad de las personas conviene tener en cuenta las recomendaciones del SEPD para evaluar la *proporcionalidad de las medidas que limitan los derechos fundamentales a la intimidad y a la protección de los datos personales*[858]. Las medidas propuestas deben ser proporcionales en la evaluación de su legalidad cuando implique tratamiento de datos personales. En la Carta de los Derechos Fundamentales, (apartado 1 del artículo 52) se establece que las medidas deben estar previstas por la ley, respetar la esencia de los derechos, responder realmente a objetivos de interés general reconocidos por la Unión o a la necesidad de proteger los derechos y libertades de los demás, ser *necesarias* y *proporcionadas*. Por su parte tal y como señala el SEPD, en la *sentencia Derechos Digitales*[859], el TJCE ha dictaminado que *el poder discrecional del legislador se ve reducido a la hora de restringir los derechos fundamentales*: "en función de una serie de factores, entre los que se incluyen, en particular, el ámbito en cuestión, la naturaleza del derecho en cuestión garantizado por la Carta, la naturaleza y la gravedad de la interferencia y el objeto perseguido por la interferencia". ¿Pero, "cuál es el alcance de la discrecionalidad (reducida) del legislador de la UE? La legislación de la UE en cuestión debe establecer *normas claras y precisas* que regulen el alcance y la aplicación de la medida en cuestión e impongan unas garantías mínimas para que las

[857] Vid. https://www.boe.es/buscar/act.php?id=BOE-A-2002-22188

[858] SEPD (25 de febrero de 2019). Directrices del SEPD para evaluar la proporcionalidad de las medidas que limitan los derechos fundamentales a la privacidad y la protección de datos personales. Recuperado de https://edps.europa.eu/data-protection/our-work/publications/guidelines/edps-guidelines-assessing-proportionality-measures_en

[859] Cfr. Asuntos acumulados C-293/12 y C-594/12, ECLI:EU:C:2014:238.

personas cuyos datos se hayan conservado dispongan de garantías suficientes para proteger de forma efectiva....” [860]. Es decir, “la necesidad implica la necesidad de una evaluación combinada, basada en hechos, de la *eficacia de la medida para el objetivo perseguido y de si es menos intrusiva en comparación con otras opciones para lograr el mismo objetivo”* o en otras palabras, “la necesidad es una condición previa para la proporcionalidad”[861]. Por lo general para el SEPD, una prueba de proporcionalidad consiste en evaluar qué *"salvaguardias"* deben acompañar a una medida *(por ejemplo, en materia de vigilancia)* con el fin de reducir los riesgos que la medida prevista supone para los derechos y libertades fundamentales de las personas afectadas a un nivel "aceptable" o proporcional.

3.2 El Reglamento eIDAS y la Directiva SRI

i. Reglamento (UE) Nº 910/2014 (eIDAS) de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

Ese Reglamento establece las condiciones en las que los ciudadanos pueden utilizar los medios de identificación electrónica reconocidos, pertenecientes a un sistema de identificación electrónica notificado de un Estado miembro, para acceder a servicios públicos en línea desde el extranjero, en particular a servicios y datos sanitarios. También establece normas sobre los servicios de confianza, como las firmas electrónicas, los sellos electrónicos y los servicios de entrega electrónica certificada, para gestionar e intercambiar de forma segura datos sanitarios minimizando el riesgo de

[860] Véase el Dictamen del SEPD 3/2017 sobre la Propuesta relativa a un Sistema Europeo de Información y Autorización de Viajes (ETIAS), pág. 13: "El SEPD duda de que el tratamiento de esta categoría especialmente sensible de datos a tan gran escala y durante este período de tiempo cumpla las condiciones establecidas en el artículo 52, apartado 1, de la Carta y, por tanto, se considere necesario y proporcionado. El SEPD cuestiona la pertinencia de la recogida y el *tratamiento de los datos sanitarios* previstos en la Propuesta debido a la falta de fiabilidad de los mismos y a la necesidad de tratarlos debido a la escasa relación entre los riesgos para la salud y los viajeros exentos de visado". Además, en el 2019, el SEPD, señala el informe AI Now Report 2018, diciembre de 2018 en el que se ha prestado especial atención a los riesgos de la Inteligencia Artificial aplicada al reconocimiento facial. Disponible en https://ainowinstitute.org/AI_Now_2018_Report.pdf. Y sobre los datos biométricos, véase el Dictamen 3/2012 del WP 29 sobre los avances en las tecnologías biométricas, páginas 30 y 31, sobre los riesgos específicos que plantean los datos biométricos; y el Dictamen 02/2012 del WP 29 sobre el reconocimiento facial en los servicios en línea y móviles, Sección 5, Riesgos específicos y recomendaciones.

[861] En los asuntos acumulados C-465/00, C-138/01y C-139/01, Rechnungshof, ECLI:EU:C:2003:294, apartado 1, letra c) del apartado 1 del artículo 2 de la Directiva. 91, el CJEU sostuvo que: "Si los órganos jurisdiccionales nacionales llegan a la conclusión de que la legislación nacional de que se trata es incompatible con el artículo 8 del Convenio, dicha legislación tampoco puede cumplir el requisito de proporcionalidad del artículo 6, apartado 1, letra c), y del artículo 7, letras c) o e), de la Directiva 95/46/CE" (negrita en el original).

posibles manipulaciones y usos indebidos. El uso de medios de identificación y autenticación electrónicas seguras previstos debería mejorar el acceso, la seguridad y la confianza respecto a los sistemas de *historiales médicos electrónicos.*

Un aspecto fundamental para garantizar la *confianza* en los intercambios de datos entre sistemas de historiales médicos electrónicos es la identificación y autenticación sólidas y fiables de todas las partes implicadas. El uso de las identificaciones electrónicas nacionales notificadas (eID) facilita la *identificación y la autenticación transfronterizas* de los ciudadanos para que puedan acceder a sus datos sanitarios con total seguridad y a su conveniencia y apoya el principio de «no repudio», que garantiza el origen y la integridad de tales datos. Mediante el reconocimiento mutuo de los sistemas nacionales de identificación electrónica previstos en el Reglamento, los ciudadanos de un Estado miembro pueden utilizar sus identificaciones electrónicas nacionales para acceder de forma segura a los servicios en línea prestados en otro Estado miembro.

ii. Directiva (UE) Nº 2016/1148 (SRI) de 6 de Julio, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión[862]

Conforme a esta Directiva[863] (y su trasposición al Real Decreto-ley de 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información), los prestadores de asistencia sanitaria considerados operadores de "*servicios esenciales*"[864] por los Estados miembros y los proveedores de servicios digitales que entran en su ámbito de aplicación están obligados a adoptar *medidas técnicas y de organización adecuadas y proporcionadas* para *gestionar los riesgos* que se planteen para la seguridad de las redes y sistemas de información que utilizan en sus operaciones de prestación de servicios. Las obligaciones de seguridad que asuman deberán ser proporcionadas al nivel de riesgo que afronten y estar basadas en una evaluación previa de los mismos.

[862] Eur-Lex. Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016L1148

[863] La citada Directiva les somete a un régimen de armonización máxima, equivalente a un reglamento, pues se considera que su regulación a escala nacional no sería efectiva por tener un carácter intrínsecamente transnacional.

[864] El Real-Decreto Ley define como "servicio esencial" al servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas, que dependa para su provisión de redes y sistemas de información.

Las normas de desarrollo del Real Decreto-Ley podrán concretar las obligaciones de seguridad exigibles a los prestadores sanitarios, incluyendo en su caso las inspecciones a realizar o la participación en actividades y ejercicios de gestión de crisis.
También están obligados a notificar a la autoridad competente o al equipo nacional de respuesta a incidentes de seguridad informática (CSIRT) los incidentes de seguridad que tengan un impacto significativo o sustancial sobre la continuidad de los servicios que prestan. Por lo que se refiere, en particular, a la ciberseguridad de los sistemas de historiales médicos electrónicos, la certificación de la ciberseguridad puede permitir demostrar que se cumplen los requisitos de ciberseguridad en el marco de ciberseguridad pertinente de la Unión.

4. EL RÉGIMEN JURÍDICO EN INVESTIGACIÓN Y DATOS PERSONALES CON FINES SANITARIOS

La investigación con personas o con sus muestras biológicas plantean inevitablemente varios desafíos a la bioética y al derecho de la protección de datos y privacidad. A priori, convendría diferenciar los siguientes tres conceptos:

Investigación biomédica	**Investigación básica y clínica no biomédica**	**Ensayos clínicos**
Utiliza como objeto principal el material biológico.	Se efectúa directamente sobre seres humanos, y no sobre sus muestras biológicas. Está relacionada con la atención sanitaria. .	Serían una subespecie del género investigación clínica, al efectuarse generalmente sobre seres humanos.
De aplicación: RGPD, LOPDGDD y LIB	*De aplicación:* RGPD, LOPDGDD, LIB y normativa Ensayos Clínicos. Normativa autonómica HC.	*De aplicación*: Ley de autonomía del paciente, Ley 29/2006, Real Decreto 223/2004, Códigos tipo Farmaindustria y RGPD, CTR.

4.1. La investigación biomédica.

Según Varcacel[865], la investigación biomédica tiene por objeto profundizar en el conocimiento de los mecanismos moleculares, bioquímicos, celulares, genéticos, fisiopatológicos y epidemiológicos de las enfermedades y problemas de salud, y establecer las estrategias para su prevención y tratamiento. Para ello, el ámbito de la investigación biomédica incluye, además, las propias disciplinas clínicas, la investigación en nuevos fármacos y desarrollos terapéuticos, la investigación en salud pública y servicios de salud, donde la epidemiología, la sociología y la economía se aplican conjuntamente (Ministerio de Ciencia y Tecnología, 2003)[866].

A la investigación biomédica le será de aplicación el RGPD, la nueva LOPDGDD y la Ley 14/2007, de 3 de julio, de Investigación Biomédica (LIB), las cuales intentaremos desarrollar a continuación.

4.1.1. RGPD e Investigación biomédica.

Como vamos a ver y señaló la AEPD en el anteriormente citado informe, "el Reglamento general de Protección de Datos no implica una alteración del marco normativo actualmente vigente en España en relación con el tratamiento de datos en el marco de la investigación biomédica". La autoridad reconoce la importancia de la investigación biomédica y sus beneficios para los individuos y la sociedad en su conjunto. Pero, además, han declarado[867] respondiendo a los temores de la comunidad científica, que no existe riesgo para la investigación puesto que el "RGPD permite que las regulaciones nacionales continúen vigentes" (Rubí, 2018) refiriéndose al sistema de garantías y excepciones.

Además, esta flexibilidad se evidencia en los considerandos 52 y 53, que hacen referencia a cómo se debe interpretar el posible uso de datos obtenidos en el ámbito de la salud. Rubí señaló que "una de las referencias específicas y novedosas que presentan

[865] Valcárcel, N. (2009). Protección de datos de salud e investigación hospitalaria. En C. Gómez-Piqueras, R. Martínez-Martínez, J. M. Pérez-Gómez, C. M., Romeo, J. Sánchez-Caro y N. Valcárcel, *Protección de datos e investigación biomédica*. Cizur Menor: Thomson Reuters Aranzadi.

[866] Ministerio de Ciencia y Tecnología (2003). *Plan Nacional de Investigación Científica, Desarrollo e Innovación Tecnológica, 2004-2007*. Madrid: Ministerio de Ciencia y Tecnología.

[867] RedaccionMédica (22 de febrero de 2018). Protección de datos: "Las enmiendas sanitarias a la LOPD no son necesarias". Recuperado de https://www.redaccionmedica.com/secciones/derecho/proteccion-de-datos-las-enmiendas-sanitarias-a-la-lopd-no-son-necesarias--7480

es que se promueve el tratamiento de datos con fines de beneficio para las personas y de la sociedad en su conjunto. Esto va a permitir que la interpretación que se haga de las finalidades en la investigación biomédica pueda ser más amplia".

4.1.1.1. Interpretación y ámbito del concepto de investigación biomédica

El Reglamento realiza una interpretación sumamente amplia del concepto de investigación científica, puesto que según su considerando 159:

> "El tratamiento de datos personales con fines de investigación científica debe interpretarse, a efectos del presente Reglamento, de manera amplia, que incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado. Además, debe tener en cuenta el objetivo de la Unión establecido en el artículo 179, apartado 1, del TFUE de realizar un espacio europeo de investigación. Entre los fines de investigación científica también se deben incluir los estudios realizados en interés público en el ámbito de la salud pública".

En este mismo sentido, el considerando 157 amplia el ámbito de la investigación, teniendo en cuenta la posible recogida de datos procedentes de registros. Así, recuerda que:

> "combinando información procedente de registros, los investigadores pueden obtener nuevos conocimientos de gran valor sobre condiciones médicas extendidas, como las enfermedades cardiovasculares, el cáncer y la depresión. Partiendo de registros, los resultados de las investigaciones pueden ser más sólidos, ya que se basan en una población mayor. Dentro de las ciencias sociales, la investigación basada en registros permite que los investigadores obtengan conocimientos esenciales acerca de la correlación a largo plazo, con otras condiciones de vida, de diversas condiciones sociales, como el desempleo y la educación. Los resultados de investigaciones obtenidos de registros proporcionan conocimientos sólidos y de alta calidad que pueden servir de base para la concepción y ejecución de políticas basada en el conocimiento, mejorar la calidad de vida de numerosas personas y mejorar la eficiencia de los servicios sociales. Para facilitar la investigación científica, los datos personales pueden tratarse con fines científicos, a reserva de condiciones y garantías adecuadas establecidas en el Derecho de la Unión o de los Estados miembros".

4.1.1.2.Finalidades y medidas.

A su vez, el artículo 89 dispone en sus dos primeros apartados lo siguiente respecto a las medidas:

> "1. *El tratamiento con* fines de archivo en interés público, *fines de investigación científica* o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del *principio de minimización* de los datos personales. Tales medidas podrán incluir la *seudonimización*, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo.

Como se establece en el informe "dichos datos podrán seguir siendo tratados en los términos establecidos en la Ley de Investigación Biomédica, a cuya habilitación legal se remitiría el artículo 9.2 j) del Reglamento General de Protección de Datos y que establece las garantías de seudonimización (en la redacción del texto "datos codificados o reversiblemente disociados") y minimización, delimitando igualmente las reglas de limitación de la finalidad en su artículo 60.2".

> 2. Cuando se traten datos personales con fines de investigación científica o histórica o estadísticos el Derecho de la Unión o de los Estados miembros podrá establecer excepciones a los derechos contemplados en los artículos 15, 16, 18 y 21, sujetas a las condiciones y garantías indicadas en el apartado 1 del presente artículo, *siempre que sea probable que esos derechos imposibiliten u obstaculicen gravemente el logro de los fines científicos y cuanto esas excepciones sean necesarias para alcanzar esos fines."*

En este apartado 2, el legislador señala la posibilidad de exceptuar los derechos de acceso, de rectificación, limitación del tratamiento y portabilidad de los datos.

Y en relación con el artículo 5.1 b) del reglamento (art. 4 antigua LOPD), siguiendo lo establecido *principio de limitación de finalidad* dispone que "de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales".

No obstante como prueba de flexibilidad del legislador, y respecto a las finalidades de la investigación hay algo a destacar muy importante y que hace hincapié la AEPD en el informe citado. De manera explícita, el legislador se refiere, precisamente al consentimiento prestado para el tratamiento de los datos con fines de

investigación científica, teniendo en cuenta el "*carácter intrínsecamente dinámico"* de dicha investigación. Así, señala que:

> "Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida. Por consiguiente, debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para la investigación científica. Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida". (Considerando 33)

Por su parte la AEPD establece que;

> "De todo ello se derivaría que los requisitos de especificidad y carácter inequívoco para la prestación del consentimiento *no deben ser interpretados* en el ámbito de la investigación científica de un *modo restrictivo,* limitado a una concreta investigación de la que se facilite toda la información disponible, sino que cabe considerar que concurren en los supuestos en los que el consentimiento se presta en relación con un determinado campo de investigación, pudiendo extenderse en el futro ese consentimiento, sin que ello lo vicie en modo alguno, incluso a "finalidades" o áreas de investigación que ni siquiera hubieran podido determinarse en el momento en que se prestó sin que sea necesario recabar un nuevo consentimiento del sujeto fuente, *teniendo en cuenta los beneficios para los individuos y la sociedad en su conjunto que pueden derivarse de tal investigación no prevista*".

La AEPD, señala que por ejemplo, no sería necesario "especificar" si el consentimiento *va dirigido a un tipo de cáncer o a las investigaciones oncológicas en general o incluso para ámbitos más extensos de investigación.* Antes del Reglamento europeo, no se podría, ya que tenía que ser de un campo de investigación concreto.

Por otro lado, y aplicando los principios del RGPD, nos encontramos con la *minimización de datos*, aplicación que puede resultar particular y delicado por dos motivos: (i) la dificultad de hacer buena investigación en salud con escasos datos y; (ii) la necesidad de incorporar datos de "calidad" para no hacer investigaciones erróneas o fallidas que no ayuden al desarrollo social e innovador del sector.

4.1.1.3. El consentimiento como base legitimadora

Ya hemos ido señalando este capítulo, que el artículo 9.1 parte del principio general de prohibición del tratamiento, al indica de datos relativos a la salud entre otros. No obstante, este principio se exceptuaría en los supuestos enumerados en el artículo

9.2, siendo especialmente relevantes a los efectos que aquí interesan las letras a) y j) del precepto, que *legitiman este tratamiento* cuando:

> "*el interesado dio su consentimiento explícito* para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado"

Y además, cuando;

> "el tratamiento *es necesario con* fines de archivo en interés público[868], *fines de investigación científica* o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado".

Ahora bien, la cuestión más controvertida tendría que ver con el alcance que debe prestarse al consentimiento prestado por el interesado para el uso de *sus datos con fines de investigación* o para que pueda tener lugar un *uso secundario con tales fines de datos asistenciales.* Ello implica que en los supuestos en que el tratamiento deba fundarse en el consentimiento, el interesado debería conocer de forma clara e inequívoca las *finalidades* para las que se procederá a dicho tratamiento. Por ello, en el consentimiento deberá cumplir los requisitos recogidos en el artículo 4.11 ("toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen").

4.1.1.4. Las otras y dobles legitimaciones

La AEPD[869] (gabinete jurídico) ya empezó a dar ciertas pautas donde señalaba que se podría hacer investigación sin consentimiento "siempre que fuera investigación de

[868] En este sentido, al Gabinete Jurídico de la AEPD, se le requirió preguntando sobre si el consentimiento sería necesario en el caso de investigación biomédica para la identificación de factores de riesgocruzando bases de datos clínicas y administrativas, gestionadas por organismos públicos (diferentes al CNE del ISCIII) o podría existir habilitación legal para la cesión de esos datos sin reqerir el consentimiento. Vid en https://www.aepd.es/media/informes/2018-0121-legitimacion-para-el-tratamiento-de-datos-en-materia-de-salud-publica.pdf

[869] También la Autoridad Catalana de protección de datos señala que el tratamiento de datos seudonimizaods para fines de investigación biomédica puede encontrar suficiente habilitación en bases jurídicas diferentes a la del consentimiento y artículo 9.2. apdo j en conexión con el art. 89. Cuando concurran las circunstancias del DA 17 2d, no será imprescindible el consentimiento de los afectados para llevar a cabo el tratamiento de los datos pseudonomizados.

interés pública", con el visto del Comité de Bioética. A mi modo de ver, cuando se habla del consentimiento como base legitimadora no siempre va "sola" sino acompañada de otras. Sería interesante señalar de una forma, más o menos clara, qué bases legitimadoras podrían acompañar al consentimiento explícito, coinvirtiéndose en "doble legitimación". Tiene sentido esto que comentamos, ya que de no contar con esa posibilidad de apertura de protección, estaríamos dejando sin sentido la intención principal del regulador de proteger a los datos personales de categoría especial como son los de salud. Por lo que a falta de un código de conducta europeo de investigación de salud y protección de datos personales[870], quizás podría ser interesante estudiar las interpretaciones que realiza el Comité Europeo de Protección de Datos respecto al Reglamento europeo de los ensayos clínicos (del que hablaremos más tarde) y procurar hacer una interpretación por analogía. El Comité señaló la necesidad e importancia de "revisar" la legitimación, ya que pueden existir situaciones donde el sujeto (también en investigación biomédica) pertenezca a un grupo desfavorecido desde el punto de vista económico o social, o en casos de dependencia institucional o jerárquica la legitimación puede resultar dudosa. Por ello, se puede recomendar optar por legitimación doble del *interés público*[871] o legimaticón de *interés legítimo*[872] , junto con la del consentimiento que en ocasiones puede resultar de dudosa legitimación o que incluso, ponga en peligro.

4.1.2. LOPDGDD e Investigación Biomédica

---

https://apdcat.gencat.cat/es/documentacio/resolucions-dictamens-i-informes/cercador/cercador-detall/CNS-15-2019-00001

[870] Como es el caso del proyecto europeo www.panelfit.eu cuyo grupo de investigación formado por profesionales e investigadores interdisciplinares de Europa, trabajan entre otras cuestiones a diseñan un posible código de conducta europeo sobre investigación en salud y protección de datos personales, en el cual tengo el gran privilegio de poder participar de forma activa. Pero no sólo a nivel comunitario existen proyectos (piloto) de códigos de conducta, sino a nivel internacional como es el caso de iniciativas de Naciones Unidas para crear un documento que marque pautas respecto a los datos de salud y los derechos funamentales de las personas, en concreto la protección de datos. El papel de las universidades en el apoyo a la creación de documentos base armonizadores en esta materia es muy importante.

[871] Vid. Art. 6.1.e RGPD (y LIB). Por Ejemplo, cuando sea resultado de un encargo por un organismo público o privado fundado en una ley nacional. La Autoridad Catalana de Protección de Datos interpreta que siempre que existan las medidas adecuadas, las bases jurídicas adecuadas serán otras que el consentimiento. El tratamiento de datos personales en el contexto de los ensayos clínicospuede considerarse necesario para la realización de una tarea realizada en la del interés público cuando la realización de ensayos clínicos entra directamente en el ámbito de aplicación del mandato, misiones y tareas encomendadas a un organismo público o privado por el Derecho de la Unión o nacional.

[872] Vid. D.A. 17ª 2. d)

Como hemos establecido, la nueva normativa europea no implica "una alteración del marco normativo actualmente vigente en España en relación con el tratamiento de datos en el marco de la investigación biomédica" [873], en todo caso permite ser más flexible en algunos aspectos como hemos destacado.[874]

Profundizando en la ley y en las modificaciones de las que hablamos, en la *disposición decimoséptima* (aptdo. 2) señala que el tratamiento de datos en la investigación en salud se regirá por los siguientes criterios:

> "a) El interesado o, en su caso, su representante legal podrá otorgar el ***consentimiento*** para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora".

Se trata del "consentimiento reforzado"; libre, específico, informado e inequívoco.

> "b) Las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional *relevancia y gravedad para la salud pública*".
>
> "c) Se considerará lícita y compatible la *reutilización de datos personales* con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento

[873] Ya señalaba Rubí (2018), antes de la entrada en vigor de la LOPDGDD, la siempre posibilidad de que en un proyecto de ley se incorpore una modificación normativa que prevea alguna perspectiva adicional. Se refería, por ejemplo, al que era por aquel momento "proyecto de ley orgánica" (si lo consideraban oportuno los grupos parlamentarios). Pero recalcaba que si se quería hacer "no es porque el proyecto de ley ni el reglamento europeo supongan una limitación adicional, sino porque se puede entender que se puede aprovechar esa coyuntura para reformular cualquier norma en general y en particular del ámbito sanitario, pero no en el sentido de que sea necesaria para garantizar el régimen jurídico vigente".

[874] Debiés, E. (2017). Apertura de datos de salud en Francia, impacto en la investigación y la Seguridad Social. *Revistas UM Bioderecho*. Núm. 5, pág. 7. Recuperado de https://digitum.um.es/xmlui/bitstream/10201/54099/1/Apertura%20de%20datos%20de%20salud%20en%20Francia%2C%20impacto%20en%20la%20investigacion%20y%20la%20seguridad%20social.pdf Por ejemplo, pongamos la mirada en otro país: Francia. Como Señala *Debíes* en 2016, se creó la ley modernización del Sistema de Salud de 26 de enero de 2016, que estableció la apertura de los datos agregados de salud para fines de investigación, estudio o evaluación de interés público para todos los ciudadanos, profesionales de la salud u organismos (públicos o privados) que participaran en el funcionamiento del sistema de salud y la atención sanitaria. Por cuanto nos interessa, hay condiciones; (i) *los tratamientos de datos no deben de tener por finalidad, ni permitir en ningún momento, la identificación de las personas*; (ii) los trabajos ejecutados a partir de los datos *no deben de conducir a la promoción de productos* dirigidos a profesionales de la salud o centros de salud, (iii) ni *permitir que se excluyan garantías de los contratos de seguro o modificar las cuotas o primas de seguros*. Además, "para tener acceso a la base, cualquier organismo de investigación o estudio que desee llevar a cabo un proyecto de interés público debe someterlo al Instituto nacional de los datos de salud. Sus miembros incluyen representantes del Estado, los usuarios de la seguridad social y los productores y usuarios públicos y privados de datos de salud. El protocolo de estudio lo validará entonces un comité científico, antes de la autorización de la CNIL tras el análisis de los aspectos relacionados con el respeto de la vida privada".

para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial.

En tales casos, los responsables *deberán publicar la información* establecida por el artículo 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, en un lugar fácilmente accesible de la *página web corporativa del centro* donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato. Para los tratamientos previstos en esta letra, se requerirá *informe previo* favorable del *comité de ética de la investigación"*.

Respecto a la *reutilización de datos*[875], el legislador destaca la necesidad de publicar la información en la página web corporativa del centro donde se realice la investigación o estudio clínico y notificar a los interesados y en todo caso, se requerirá del informe previo favorable del comité de ética de la investigación.

"d) Se considera lícito el uso de *datos personales seudonimizados* con fines de investigación en salud y, en particular, biomédica. El uso de datos personales seudonimizados con fines de investigación en salud pública y biomédica requerirá:

1.º Una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación.

2.º Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando:

i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.

ii) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados.

875 Por otro lado, el legislador se refiere en la disposición transitoria sexta a la *reutilización con fines de investigación en materia de salud y biomédica de datos personales recogidos con anterioridad a la entrada en vigor de la LOPDGDD.* Señalándose que "se considerará lícita y compatible la reutilización con fines de investigación en salud y biomédica de datos personales recogidos lícitamente con anterioridad a la entrada en vigor de esta ley orgánica cuando concurra alguna de las circunstancias siguientes: a) Que dichos datos personales se utilicen para la finalidad concreta para la que se hubiera prestado consentimiento. b) Que, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen tales datos para finalidades o áreas de investigación relacionadas con la especialidad médica o investigadora en la que se integrase científicamente el estudio inicial".

> Podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria.

La seudonimización es una técnica de tratamiento de los datos personales por la que no se puede reconocer la identidad de una persona sin utilizar información adicional (reidentificación). Se trata de un método cuya finalidad es disminuir el vínculo que hay, lo máximo posible, entre los datos y el titular de datos de salud. Los datos "seudonimizados" seguirán siendo de carácter personal y por ello, seguirán estando sujetos al cumplimiento del RGPD. Los datos anonimizados no podrán conectarse con la persona a la que pertenecen, no se consideran datos personales y no están sometidos al RGPD. Para determinar si una persona es inidentificable han de utilizarse "todos los medios que puedan ser razonablemente utilizados y sin esfuerzos desproporcionados". Podemos evidenciar el esfuerzo por el legislador nacional para proteger a los titulares de la *reidentificación* en el caso de los datos anonimizados o pseudonimizados.

> "e) Cuando se traten datos personales con fines de investigación en salud, y en particular la biomédica, a los efectos del artículo 89.2 del Reglamento (UE) 2016/679, podrán *excepcionarse* los derechos de los afectados previstos en los artículos 15, 16, 18 y 21 del Reglamento (EU) 2016/679 cuando:
>
> 1.º Los citados derechos se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados o seudonimizados.
>
> 2.º El ejercicio de tales derechos se refiera a los resultados de la investigación.
>
> 3.º La investigación tenga por objeto un interés público esencial relacionado con la seguridad del Estado, la defensa, la seguridad pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley".
>
> "f) Cuando conforme a lo previsto por el artículo 89 del Reglamento (UE) 2016/679, se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica se procederá a:
>
> 1.º Realizar una *evaluación de impacto* que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del Reglamento (UE) 2016/679 o en los establecidos por la autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos.

2.º Someter la investigación científica a las *normas de calidad* y, en su caso, a las directrices internacionales sobre *buena práctica clínica*.

3.º Adoptar, en su caso, *medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados.*

4.º Designar un *representante legal* establecido en la Unión Europea, conforme al artículo 74 del Reglamento (UE) 536/2014, si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con el previsto en el artículo 27.1 del Reglamento (UE) 2016/679".

El legislador refuerza el derecho a la protección de datos del titular de datos personales en el contexto de la investigación exigiendo a los investigadores la realización de una evaluación de impacto (Art.35 RGPD) donde se incluye detalle y análisis del riesgo de la "reidentificación" de los datos anonimizados o pseudonimizados. Pero no sólo eso, sino que deberán adoptar medidas concretas y nombrar un representante legal si el promotor del ensayo clínico no está en la UE.

"g) El uso de datos personales seudonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido al informe previo del *comité de ética de la investigación* previsto en la normativa sectorial.

En defecto de la existencia del mencionado Comité, la entidad responsable de la investigación requerirá informe previo del delegado de protección de datos o, en su defecto, de un experto con los conocimientos previos en el artículo 37.5 del Reglamento (UE) 2016/679"

"h) En el plazo máximo de un año desde la entrada en vigor de esta ley, los comités de ética de la investigación, en el ámbito de la salud, biomédico o del medicamento, *deberán* integrar entre sus miembros un delegado de protección de datos o, en su defecto, un experto con conocimientos suficientes del Reglamento (UE) 2016/679 cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados".

Por otro parte, el legislador nacional no pierde la oportunidad de resaltar la importancia y la obligación de integrar un DPO en el comité de ética cuando existan actividades que comporten tratamiento de datos personales seudonimizados o anonimizados.

En definitiva, "la nueva Ley Orgánica flexibiliza el tratamiento de datos para la *investigación en salud y; (i) amplía las finalidades* para las que se puede otorgar el consentimiento al tratamiento; (ii) recoge la posibilidad de *reutilizar* la información sobre la que se ya se haya prestado consentimiento con anterioridad; (iii) recoge el uso

de datos *pseudonimizados*[876] como una opción para facilitar la investigación sanitaria incluyendo garantías para evitar la reidentificación de los afectados; (iv) regula las garantías de este tratamiento, incluyendo la intervención de los *Comités de Ética de la Investigación* o, *en su defecto, del Delegado de Protección de Datos* o *de un experto en protección de datos personales*"[877].

En conclusión, tanto el RGPD como la LOPDGDD "mantienen inalterado el régimen contenido en la normativa reguladora de la investigación biomédica" y además, "permiten realizar una interpretación más flexible del alcance que puede darse al consentimiento prestado de conformidad con la misma, superando, a título de ejemplo, la interpretación más restrictiva contenida en el artículo 60 de la Ley de Investigación Biomédica". Esta interpretación sería la que se debería tomar por parte de los comités de investigación. En el próximo apartado trataremos entre otras cuestiones, la investigación sanitaria en el marco de proyectos de *big data* y profundizaremos sobre las novedades normativas y sus implicaciones.

4.1.3. Ley 14/2007, de 3 julio, de Investigación Biomédica (LIB).

Respecto a investigación biomédica se aplicará, en particular, su art. 5 y 46 y ss., cuando tenga por objeto:

1. Las investigaciones relacionadas con la salud humana que impliquen procedimientos invasivos.
2. La donación y utilización de ovocitos, espermatozoides, preembriones, embriones y fetos humanos o de sus células, tejidos u órganos con fines de investigación biomédica y sus posibles aplicaciones clínicas.
3. El tratamiento de muestras biológicas, su movimiento y su almacenamiento en biobancos.
4. La realización de análisis genéticos y el tratamiento de datos genéticos de carácter personal.
5. La investigación biomédica básica y clínica.

Por su parte, el artículo 5 de esta Ley establecía concretamente que:

> "1. Se garantizará la *protección de la intimidad personal y el tratamiento confidencial de los datos personales* que resulten de la actividad de *investigación biomédica,* conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección

[876] Se trata de información a partir de la cual los identificadores han sido eliminados o transformados pero indirectamente los identificadores permanecen intactos. Por ejemplo, *Jane Smith, Diabetes, HgB 15,1 G / dl = Csrk123.*

[877] AEPD. Novedades para el Sector Privado. Recuperado de https://www.aepd.es/media/docs/novedades-lopd-sector-privado.pdf

de Datos de Carácter Personal. Las mismas garantías serán de aplicación a las muestras biológicas que sean fuente de información de carácter personal.

2. La *cesión de datos de carácter personal a terceros* ajenos a la actuación médico-asistencial o a una investigación biomédica, requerirá el *consentimiento expreso y escrito del interesado*.

En el supuesto de que los datos obtenidos del sujeto fuente pudieran revelar información de carácter personal de sus familiares, la cesión a terceros requerirá el consentimiento expreso y escrito de todos los interesados.

3. Se *prohíbe la utilización* de datos relativos a la salud de las personas con fines distintos a aquéllos para los que se prestó el consentimiento. (Una vez analizadas todas las normativas, llama la atención como esta interpretación más estricta es sustituida por una algo más amplia del RGPD).

4. Quedará sometida al *deber de secreto* cualquier persona que, en el ejercicio de sus funciones en relación con una actuación médico asistencial o con una investigación biomédica, cualquiera que sea el alcance que tengan una y otra, acceda a datos de carácter personal. Este deber persistirá aún una vez haya cesado la investigación o la actuación.

5. *Si no fuera posible publicar* los resultados de una investigación sin identificar a la persona que participó en la misma o que aportó muestras biológicas, tales resultados *sólo* podrán ser publicados cuando haya mediado el *consentimiento previo y expreso* de aquélla."

En definitiva, tal y como recalca el informe de la AEPD (2018)[878]; "el modelo establecido en el actualmente vigente en materia de investigación biomédica parte, como regla general del consentimiento del sujeto fuente, que no obstante podrá quedar *exceptuado* en determinados supuestos, bien por *no ser posible la identificación* del sujeto por haber sido anonimizados sus datos conforme al artículo 3 i), previo dictamen favorable del Comité Ético de Investigación, bien *cuando se trate de una investigación relacionada con la inicial*, al considerarse el fin de dicha investigación compatible con el de aquélla en que se prestó el consentimiento. Fuera de estos casos sería, en términos de la Ley, necesario el consentimiento expreso del afectado (artículo 58.1 LIB) para una investigación concreta (artículo 60.1 LIB)".

[878] AEPD. Informe 073667/2018 del Gabinete Jurídico. Recuperado de https://www.aepd.es/media/informes/2018-0046-investigacion-biomedica.pdf

4.1.3.1.Datos genéticos.

Resulta de interés, destacar las particularidades de los *datos genéticos* habida cuenta su presencia en estos escenarios de investigación biomédica. En primer término, el art. 4.5 LIB proclama el derecho de la *persona a ser informada de sus datos genéticos* y otros de carácter personal que se obtengan en el curso de una investigación biomédica, según los términos en que manifestó su voluntad. El mismo derecho se reconoce a la persona que haya aportado, con la finalidad indicada, muestras biológicas, o cuando se hayan obtenido otros materiales biológicos a partir de aquellos. A continuación, el art. 4.6 dispone que se respetará el derecho de la persona a *decidir que no se le comuniquen* los datos a los que se refiere el apartado anterior, incluidos los descubrimientos inesperados que se pudieran producir. No obstante, cuando esta información, según criterio del médico responsable, sea necesaria para evitar un grave perjuicio para su salud o la de sus familiares biológicos, se informará a un familiar próximo o a un representante, previa consulta del comité asistencial si lo hubiera. En todo caso, la comunicación se limitará exclusivamente a los datos necesarios para estas finalidades. Los análisis genéticos con fines de investigación biomédica o la utilización de los datos provenientes de los mismos solo podrán ser realizados cuando el sujeto interesado haya prestado expresamente su consentimiento, o cuando dichos datos hayan sido previamente anonimizados.

4.1.3.2.Muestras biológicas.

Como señala Romeo (2009), "la muestra biológica identificada o vinculada a una persona merece la especial protección que la LOPD otorga a los demás datos de carácter personal relativos a la salud". En consecuencia, el régimen jurídico de la muestra biológica es análogo al de los datos de carácter personal, incluidas las facultades, derechos y deberes que se reconocen a las partes que puedan guardar relación con ellos, incluidos los titulares de los datos (sujetos fuente).

Respecto a la información previa al uso de la muestra biológica, la LIB (Art. 59) dispone que sin perjuicio de lo establecido en la legislación sobre protección de datos, antes de que el sujeto fuente emita su consentimiento, deberá recibir cierta información por escrito como la finalidad de la investigación o línea de investigación, beneficios esperados, posibles inconvenientes con la donación y obtención de la muestra, identidad

del responsable de la investigación, derecho de revocación del consentimiento y sus efectos, lugar de realización del análisis y destino de la muestra, garantía de confidencialidad, advertencia sobre la posibilidad de que se obtenga información relativa a su salud, advertencia de la implicación de la información que se pudiera obtener para sus familiares y la conveniencia, indicación de la posibilidad de ponerse en contacto con el sujeto fuente[879].

Además, en el caso de la investigación con células y tejidos destinados a su aplicación en el ser humano, los datos para garantizar la trazabilidad *deben conservarse durante al menos treinta años*.

4.2. Investigación clínica no biomédica

La investigación clínica que no utiliza como objeto principal tejidos o muestras biológicas (o los datos genéticos procedentes de los mismos), sino que se desarrolla directamente sobre pacientes (pues la investigación sobre sujetos no enfermos y voluntarios se considera investigación no clínica), se desarrolla indisolublemente unida a la atención sanitaria; tanto los investigadores que la llevan a cabo (médicos, odontólogos, personal de enfermería o fisioterapia) como los centros en los que se desarrolla (hospitales y centros de atención primaria) cuentan entre sus funciones, además de la puramente asistencial, la docente y la investigadora.

Será de aplicación los principios de la LIB, las normas generales de protección de datos personales de RGPD y las normas estatales y autonómicas sobre historias clínicas. Ahora bien, los investigadores clínicos disponen de dos opciones para recoger datos personales para investigar:

a.) Obtener el consentimiento del paciente
b.) Tratar la información de manera disociada, separando los datos identificativos de los de carácter clínico-asistencial.

Ahora bien, no siempre es fácil conseguir el consentimiento o disociar los datos; ¿cómo obtener los datos personales de un paciente para conseguir su consentimiento?

4.2.1. Utilización de datos anonimizados

[879] Y además, para los sujetos fuentes cuyas muestras serán anonimizadas (y por tanto, no sujetas a la legislación en materia de protección de datos), el sujeto fuente recibirá información sobre la finalidad de la investigación o línea de investigación, beneficios esperados, posibles inconvenientes y la identidad del responsable de la investigación.

La solución que da la legislación es como venimos diciendo que, en primer lugar, los datos anonimizados no requieren de consentimiento al no poder asociarse esa información con personas identificadas o identificables.

4.2.2. Utilización datos personales

y en segundo lugar, en el caso de la utilización de los datos personales para uso administrativo en la atención primaria u hospitalaria con fines de investigación es posible siempre que se obtengan para contactar con los titulares al objeto de obtener su consentimiento en cualquier actividad investigadora. No obstante, se deberían cumplir algunas cuestiones para el *tratamiento de datos personales* como;

a.) Autorización del responsable del fichero. Sólo él podrá contactar con sus titulares.
b.) El fichero se deberá entregar al investigador principal o persona responsable de la investigación.
c.) En caso de cartas, deberán estar firmadas por el órgano competente y el investigador. Si el contacto se realiza por teléfono será necesario un compromiso de confidencialidad por parte de la persona que llama.
d.) No es posible dar los datos a un tercero para que sea quien contacte salvo que haya por medio un contrato de encargo de tratamiento, donde realice el trabajo en nombre y por cuenta de la institución sanitaria pública.

4.2.3. Utilización de datos de HC.

Y en tercer lugar, en el caso de la utilización de datos obtenidos de historias clínicas, se deberá realizar un proceso de anonimización que permita obtener los datos clínicos de interés, separándolos de los identificativos (por ej. con mecanismos informáticos de extracción selectiva). Y de no ser posible, se deberá pedir el consentimiento informado de los sujetos fuente de acuerdo con la legislación vigente.

4.2.4. Cesión de datos a investigadores.

En ocasiones, se puede dar que participen diferentes instituciones, entidades u organizaciones (públicas y privadas) incluso de diferentes países, por lo que se requiere contar con las mayores garantías posibles en el tratamiento y cesión de datos a los

investigadores. Se entiende que el equipo cedente deberá obtener el consentimiento de los interesados que habrá de ser expreso para poder realizar esta cesión. Además deberá existir un contrato de encargo de tratamiento (Art. 28.3 RGPD) entre ambos equipos:

Además, al margen del régimen jurídico en materia de protección de datos, los protocolos jurídicos o procedimientos técnicos deberán ser conocidos por ambos equipos. Y serán los equipos de investigación y los centros responsables, responsables únicos o solidarios, en función del tipo de acción posible ejercitada por el perjudicado y el alcance de negligencia de cada uno. Y es por ello, que parecería inviable asignar, a priori, distribución de carga de responsabilidades de general aplicación.

4.3. Ensayos clínicos.

El Real Decreto 223/2004 define el ensayo clínico como "toda investigación efectuada en seres humanos para determinar o confirmar los efectos clínicos, farmacológicos y/o demás efectos farmacodinámicos, y/o de detectar las reacciones adversas, y/o de estudiar la absorción, distribución, metabolismo y excreción de uno o varios medicamentos en investigación con el fin de determinar su seguridad y/o su eficacia". Para estudiar las obligaciones de los investigadores y los derechos de los sujetos fuente, previamente debemos enumerar los sujetos participantes en cualquier ensayo clínico:

Promotor	**Monitor**	**Investigador**	**Comité ética (CEIC)**	**Sujeto Fuente**
Individuo, empresa o institución u organización responsable del inicio, gestión y/o financiación	Profesional capacitado con competencia clínica, elegida por el promotor, que se encarga del seguimiento directo de la realización del ensayo. Sirve de vínculo entre	Médico o persona con formación científica y de su experiencia en atención sanitaria. Pueden denominarse investigadores principales	Organismo independiente formado por profesionales sanitarios y no sanitarios, encargados por velar por la protección de los derechos, seguridad y bienestar de los sujetos que participan en un ensayo y que ofrecen una garantía pública mediante un dictamen sobre el protocolo del ensayo, la idoneidad de los investigadores, la adecuación de las instalaciones,	Es el individuo que participa en el ensayo clínico, bien recibiendo el medicamento en investigación, bien como control.

	promotor e investigador principal.	cuando hay equipos.	métodos y documentos para informar a los sujetos con el fin de obtener su consentimiento	

Ahora bien, veamos las obligaciones y derechos de éstos según el Reglamento de ensayos clínicos:

Promotor	**Investigador**	**Sujeto fuente**
Tiene responsabilidad de archivar la documentación del ensayo. Se le atribuye la figura del "responsable de fichero" (concepto derogado) al igual que la obligación derogada de notificarlo a la AEPD. También tiene la responsabilidad de elaborar informes finales o parciales del ensayo y comunicarlos a quien corresponda. Pero éstos no contienen datos personales, por lo que esa información no estaría sujeta a normativa de protección de datos.	Tiene derecho a conocer los datos personales de los sujetos a través de la documentación (a través del historial clínica). Se trataría de una codificación cuyo código solo sería conocido por el investigador de forma que no puedan los demás asociarlo con una persona identificada o identificable. Es responsable de la recogida, registro y notificación correcta y veraz de los datos del ensayo.	Deberá prestar su consentimiento previo a la recogida y tratamiento de datos, debiendo ser informado de la existencia del fichero, la identidad y dirección del responsable del tratamiento, de la finalidad de la recogida y de los destinatarios posibles. También deberá ser informado de

Según la AEPD[880](2000), la escasa información que cuenta el promotor no lleva implícita una verdadera y completa disociación ya que los pacientes podrían ser identificados con los datos del fichero.

4.3.1. RPGD y ensayos clínicos

Como señala la Junta Europea de Protección de Datos [881], "el propósito de un ensayo clínico es recopilar datos fiables y sólidos sobre una investigación de un medicamento.

[880] Agencia Española de Protección de Datos (2000). *Memoria 2000*. Madrid: AEPD. Pág 37.Recuperado de https://www.aepd.es/media/memorias/memoria-AEPD-2000.pdf . En el cual se detalla; "La existencia de un número de código en estos Cuadernos de Recogida de Datos podría suponer un nexo de unión con la historia clínica del paciente, lo que le hace identificable y por lo tanto que el fichero esté incluido en el ámbito de aplicación de la Ley".

Este principio fundamental se ve confirmado por la letra b) del artículo 3 de la Directiva[882] de ensayos clínicos[883] (CTR)". Por su parte, lo que se pretenderá con el RGPD, es distinguir los tratamientos puramente relacionados con actividades de investigación de las operaciones de tratamiento relacionadas con la protección de la salud, al tiempo que se establecen normas de calidad y seguridad para los medicamentos mediante la generación de datos fiables y sólidos. En este sentido, según el SEPD, se pueden distinguir dos tipos de tratamiento principales:

1. *Operaciones de tratamiento relacionadas con la fiabilidad y la seguridad* (o protección de la salud)

Los tratamientos necesarios para el cumplimiento de una obligación legal de que el responsable del tratamiento puede estar justificado con arreglo al artículo 6. 1. c RGPD. El marco legal las obligaciones a las que están sujetos el promotor y/o el investigador podrán ser expresamente previstos en el CTR y en las disposiciones pertinentes de la

[881] SEPD. Junta Europea de Protección de Datos. (23 de enero de 2019) . Dictamen 3/2019 relativo a las preguntas y respuestas sobre
la interacción entre el Reglamento sobre ensayos clínicos (CTR) y el Reglamento General de Protección de Datos (RGPD) (Art. 70.1.b)).Recuperado de https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf.
Estas preguntas y respuestas se crean sobre todo ante la percepción de ciertas contradicciones entre el RGPD y el CTR, en particular en relación con la base legal como el uso del consentimiento y el uso adicional de datos de ensayos clínicos.

[882] Directiva 2001/20/CE del Parlamento Europeo y del Consejo, de 4 de abril de 2001, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros sobre la aplicación de buenas prácticas clínicas en la realización de ensayos clínicos de medicamentos de uso humano. El objetivo general de la normativa era lograr un mercado interior armonizado en lo que se refiere a ensayos clínicos y medicamentos de uso humano, partiendo de un nivel elevado de protección de la salud y estableciendo al mismo tiempo normas elevadas de calidad y seguridad para los medicamentos garantizando que los datos generados en los ensayos clínicos sean fiables y sólidos.

[883] En el Dictamen 3/2019, se señala: "De este principio básico se deriva la obligación del patrocinador/investigador de seguir los siguientes pasos protocolo aprobado y los principios de buenas prácticas clínicas (artículo 47 del CTR). Además, el CTR refuerza ciertas medidas que requieren que el patrocinador/investigador registrar, procesar, almacenar y manejar los datos de tal manera que puedan ser reportados con precisión,interpretado y verificado, preservando al mismo tiempo la confidencialidad de los registros y requiriendo medidas técnicas y organizativas adecuadas para proteger la información y los datos personales (Artículo 56 del RTC). Además, el patrocinador está legalmente obligado por el CTR a llevar a cabo una serie de actividades (incluidos los que se detallan en el capítulo VIII del CTR), por ejemplo: (i) comunicar los resultados de dicho ensayo (artículo 37, apartados 4 y 8, del CTR); (ii) realizar los informes de seguridad (Artículos 41-43 del CTR); y (iii) archivar el expediente principal de los ensayos clínicos durante 25 años y los expedientes médicos de los sujetos para el plazo establecido por la legislación nacional (artículo 58 del RRC). El promotor está sujeto a las inspecciones de los Estados miembros (artículo 78 del RCC) en el contexto de que el PCG de los Estados miembros los inspectores tienen derecho a acceder a los datos de los ensayos clínicos (artículo 24 de la Directiva 2005/28/CE y el artículo 10, apartado 2, del Reglamento de aplicación de la Comisión (UE). 2017/556) y en este último Reglamento, también las historias clínicas individuales. El protocolo del ensayo clínico, autorizado por el CTR, define los objetivos y las condiciones para qué datos de los sujetos del ensayo clínico serán procesados"

Unión y nacionales. Este es el caso, por ejemplo, de las obligaciones relacionadas con el cumplimiento de las *normas de seguridad* de conformidad con los artículos 41 a 43 del CTR, y las obligaciones relativas al archivo del *expediente principal* del ensayo clínico (25 años con arreglo al artículo 58 del RCC) y los expedientes médicos de (que será determinado por la legislación nacional con arreglo a la misma disposición).
La correspondiente condición apropiada para el tratamiento legal de categorías especiales de datos en el contexto de estas obligaciones será el artículo 9, apartado 2, letra i): "El procesamiento es necesario por *razones de interés público* en el ámbito de la salud pública, como [...] garantizar un *alto nivel de calidad y la seguridad* de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base de la legislación de la Unión Europea o la legislación de un Estado miembro, que prevé medidas adecuadas y específicas para salvaguardar el derechos y libertades del interesado, en particular el secreto profesional".

2. Operaciones de tratamiento relacionadas únicamente con actividades de investigación (o investigación científica).

Éstas, por el contrario, no pueden derivarse de una obligación legal. Para que sea lícito el tratamiento en ensayo clínicos se debería basar en:

a. *Una misión de interés público* con arreglo a la letra e) del apartado 1 del artículo 6, en relación con el artículo 9, apartado 2, letras i) o j), del RGPD. El Reglamento sobre ensayos clínicos define por ley determinadas actividades de tratamiento, que sean necesarias para el cumplimiento de una misión de interés público para los propósitos descritos en el protocolo del ensayo clínico aprobado, en este caso, para perseguir los siguientes objetivos el interés público general de la Unión en la *protección de la salud pública.*
b. *Los intereses legítimos* del responsable del tratamiento con arreglo a la letra f) del apartado 1 del artículo 6, en relación con la letra j) del apartado 2 del artículo 9 del RGPD[884].

[884] No todas las situaciones de realizaciones de ensayos clínicas están bajo el paraguas de la "necesidad por interés público" del responsable del tratamieno, sino que en ocasiones puede estar dentro del paraguas de "intereses legítimos" del responsable o de un tercero, salvo cuando tales intereses legítimos los intereses están por encima de los intereses o de los derechos y libertades fundamentales de los datos sujeto" con arreglo al artículo 6.1.f del RGPD.

c. *El consentimiento expreso del interesado* con arreglo a la letra a) del apartado 1 del artículo 6 y a la letra a) del apartado 2 del artículo 9 del RGPD. Como hemos dicho reiteradas veces, el consentimiento en el caso de los datos sanitarios debe ser explícito (9.2.a RGPD) y no supondrá un fundamento jurídico válido cuando exista un desequilibrio evidente entre el interesado y el responsable del tratamiento (pensemos en posibles desequilibrios de poder entre el patrocinador/investigador y los participantes). El CTR expresamente se ocupa de estos riesgos y exige que el investigador tenga en cuenta todos los factores pertinentes circunstancias, en particular si el sujeto potencial pertenece a un grupo de interés económico o *en situación de desventaja social*, o se encuentra en una situación institucional o jerárquica dependiente que podría influir de manera inapropiada en su decisión de participar. Como señalaba el GT29, *el consentimiento no siempre se considera el fundamento jurídico más adecuado.*

Respecto al *uso secundario* de los datos fuera del protocolo en ensayos, *Van Quanthem*[885], señala que la Junta ahora reconoce específicamente que éste uso "no siempre debe requerir un nuevo consentimiento". Añade acertadamente que, "en cambio, tal uso también podría basarse en la presunción de compatibilidad en el art. 5.1.b. RGPD ("principio limitación de la finalidad") (excepción a la prohibición de tratamientos ulteriores cuando se trate de investigación científica). La aplicación de esta presunción significa que no se requiere una nueva base legal (y, por lo tanto, no hay un nuevo consentimiento de RGPD). Esta es una aclaración útil, ya que esta disposición específica en el RGPD destinada a fomentar la investigación científica a menudo se ignora".

Por último, me parece interesante señalar la importancia de definir los roles de los sujetos jurídicos intervinientes en el ámbito de los ensayos clínicos, habida cuenta el escenario de los múltiples responsables, encargados e incluso, subencargados (piénsese en corresponsables como un hospital y un promotor/investigador y un tercero que puede

885 Van Quathem K. (13 de febrero de 2019). *El Consejo Europeo de Protección de Datos publica una guía sobre la intersección del GDPR y el Reglamento de ensayos clínicos*. Recuperado de https://www.insideprivacy.com/eu-data-protection/european-data-protection-board-releases-guidance-on-intersection-of-the-gdpr-and-the-clinical-trials-regulation/

ser un monitor de ensayos), diferenciando las obligaciones contractuales entre ellos de la base jurídica del tratamiento[886].

4.3.2. LOPDGDD y ensayos clínicos.

A tener en cuenta, en el segundo apartado de la disposición XVII (tratamientos de datos de salud), se señala que: "El tratamiento de datos en la investigación en salud se regirá por los siguientes criterios: 4.º *Designar un representante legal* establecido en la Unión Europea, conforme al artículo 74 del Reglamento (UE) 536/2014, *si el promotor de un ensayo clínico no está establecido en la Unión Europea*. Dicho representante legal podrá coincidir con el previsto en el artículo 27.1 del Reglamento (UE) 2016/679".

5. PARTICULARIDADES JURÍDICAS PARA PROYECTOS DE BIG DATA E INVESTIGACIÓN BIOMÉDICA

El tratamiento y la explotación de grandes volúmenes de información a través de herramientas tecnológicas pueden ofrecer múltiples beneficios a la sociedad como lo se produce en el campo de la investigación biomédica, pero todo ello, siempre que se respete los derechos de las personas, su privacidad y la protección de sus datos personales, máxime si se refiere a una categoría de datos especiales como son la salud.
A priori, si ponemos el punto de mira en un contexto de investigación biomédica a nivel de *agencias públicas* (y no sólo públicas, diría) podemos identificar algunas particularidades técnicas como son: (i) la dificultad de gestionar grandes volúmenes de datos disponibles, el almacenamiento y la capacidad de explotación; (ii) la necesidad de programas como *algoritmos informáticos y estadísticos*, (iii) la *heterogeneidad de la información con* naturaleza genómica, clínica, biológica, etc., sus diferentes formatos (texto, valores, imágenes, genómicos) y; (iv) su dispersión a través de diferentes

[886] Cfr. Autoritad Catalana de Protección de Datos. (11 de enero de 2019). Resolución CNS 59/2018. Recuperado de http://apdcat.gencat.cat/web/.content/Resolucio/Resolucions_Cercador/Dictamens/Documents/ca_cns_2018_059.pdf

sistemas de información de grupos de hospitalarios, laboratorios de investigación, bases de datos públicas[887].

Habida cuenta estas particularidades propias con las implicaciones que suponen el avance tecnológico, se torna necesario analizar a continuación cuestiones como el origen de los datos, las finalidades, los derechos de los interesados, legitimación, las decisiones automatizadas en el contexto de la investigación, principios, evaluación de impacto, medidas técnicas y organizativas y buenas prácticas en general recomendadas por AEPD-ISMS.

5.1. Origen de los datos

Según el informe "*Código de buenas prácticas en protección de datos para proyectos de Big Data*" [888] creado conjuntamente entre AEPD e ISMS Fórum; "el origen de datos es el primer aspecto que debe tenerse en cuenta en la cadena de tratamientos contemplados en un sistema de Big Data[889]". Más si cabe, en los casos en los que se alimenta de información de varios orígenes de datos, lo que haría que según el nivel de confiabilidad que ofrezcan éstos, "la calidad de los *datos primarios* puede quedar comprometida de inicio y arrastrarse durante todo su ciclo de vida"[890].

---

[887] En Francia, como señala la autora Debiés, existen lo que se denomina *"cohorte"* que es un "grupo de personas que comparten una serie de características comunes que los investigadores siguen durante un tiempo considerable para identificar la ocurrencia de eventos de salud (enfermedad o disfunción del cuerpo) y los factores de riesgo o de protección correspondientes". Por ejemplo, están la *cohorte Constances* incluirá en el futuro 200.000 adultos entre 18 a 69 años seguidos por la Seguridad Social o La *cohorte I-Share* incluirá 30.000 estudiantes universitarios seguidos durante 10 años o el *Observatorio Mavie* que estudia los accidentes de vida cotidiana en más de 25.000 voluntarios internautas.

[888] AEPD-ISMS Forum. Código de buenas prácticas em Protección de Datos para proyectos Big Data. Recuperado de https://www.aepd.es/media/guias/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf

[889] En el informe «Big data en salud digital» ya citado, se señala que esta tecnología permite tres tipos principales de análisis; *modelos predictivos* **(**analizan los resultados anteriores para evaluar qué probabilidad tiene un individuo de mostrar un comportamiento específico en el futuro con el fin de mejorar la eficacia); *modelos descriptivos (*describen las relaciones entre los datos para poder clasificar a los individuos en grupos); y *modelos de decisión***.**

[890] Cuando hablamos de orígenes podemos referirnos a las fuentes de información y a su clasificación. En concreto, se encuentran, por un lado, las fuentes endógenas (circunscritas a la definición y control de la propia organización) y por el otro, las exógenas (o fuentes externas). Esta convivencia de las diferentes fuentes provocará la necesidad de aplicar filtros y controles compensatorios en mayor o menor medida. Aunque no siempre es fácil esta operación a pesar de las técnicas de depuración, y puede obligar a recurrir a *otros datos complementarios* para ayudar a garantizar la fiabilidad de los datos. Para evitar la desconfianza de la validez de los datos y estas barreras, cada vez más, se obtienen un mayor número de *metadatos*.

Es de interés por cuanto concierne también a los proyectos de *big data y eHealth*, conocer la clasificación de *Sunil Soares* (2012) bajo el concepto de los orígenes de datos.

Generados por humanos	**Biometría**	**Máquina a máquina**	**Grandes transacciones**	**Web y Social Media**
- Grabaciones de voz en un "call center" -Correo electrónico -Registros médicos electrónicos - Documentos en papel, notas de los profesionales sanitarios.	-Reconocimiento facial -Escáner de retina Huellas dactilares -Presión arterial, el pulso y lecturas de oximetría -Información genética	-Contadores inteligentes (lectura de sensores) - Lecturas RFID -Señales de Geolocalización	-Peticiones de atención médica -Registros de metadatos de telecomunicaciones -Registros de facturación (en formatos semiestructurados o estructurados)	-Historial de navegación - Tuits publicados - Publicaciones en el muro de Facebook -Contenido de una Web (de salud) -(Apps smartphone)

Imagen70. Tabla con orígenes de datos en big data de salud.

5.1. Finalidades

El *"principio de finalidad"* es muy importante como garantía al interesado, la cual debe ser determinada, explícita y legítima para que puedan obtener los datos.

Según el *código de buenas prácticas en protección de datos para proyectos de Big Data*[891], se considera que este principio puede suponer una barrera ya que no siempre se conoce desde el momento cero el alcance del proyecto. De cualquier modo, los datos personales no podrán usarse para finalidades "incompatibles", lo que no quiere decir que "diferentes"[892]. Un ejemplo de *big data* sanitario que ya está en fase de prueba de campo en la sanidad española es el *proyecto Hikari*[893], sobre aplicación del *big data* en salud mental. Mediante un análisis avanzado de datos se trata de valorar y prevenir el riesgo de suicidio[894] y comportamientos violentos (episodios de agravamiento de salud mental, crisis psicóticas…). Se persigue un diagnóstico más correcto y prescribir un tratamiento más adecuado.

5.2.1. Finalidad estadística.

[891] *Supra cit.*

[892] En el *dictamen WP 203* se analizan casos en los que se tratan datos posteriormente a la finalidad original donde se deberán seguir unos concretos criterios: (i) "Que exista relación entre la finalidad original y la/s posterior/es. (ii) Que el tratamiento posterior encuentre expectativas razonables del interesado.(iii) Que se tenga en cuenta la naturaleza y sensibilidad de los datos. (iv) Que se considere el impacto que puede tener en los interesados. (v) Que se analicen y se apliquen directamente medidas organizativas y técnicas como la encriptación, seudonización, separación funcional, transparencia[892], oposición al tratamiento".

[893] Vid. http://unidaddeinnovacion.shealth.eu/oferta-tecnologica/25-software/159-hikari

[894] García, J. (19 de noviembre de 2017). La Inteligencia Artificial ha evitado que me suicidara. *El País. La Retina.* Recuperado de https://retina.elpais.com/retina/2017/11/17/innovacion/1510908438_438297.html

El RGPD la define como cualquier operación de recogida y tratamiento de datos personales necesarios para la producción de resultados estadísticos. En el informe de la AEPD-ISMS, se indica que esto "implica que el resultado del tratamiento con fines estadísticos no sean datos personales, sino *datos agregados*, y que este resultado no se utilice para respaldar medidas o decisiones relativas a personas físicas concretas"[895]. Además, "se establece que los fines estadísticos *no* se *considerarán incompatibles* con los fines iniciales, si bien el Reglamento menciona que el responsable debe incluir *garantías adecuadas* en el tratamiento que aseguren que se aplican medidas técnicas y organizativas para garantizar que no se puede identificar a los interesados. Lo mismo cabe decir de otras finalidades relacionadas con Big Data tales como la *científica*[896] *o de innovación*[897] donde se ofrece una regulación favorable en estos mismos términos".

5.2. Derechos de los interesados.

Habida cuenta los derechos de los interesados explicados a lo largo de este capítulo, a continuación, quisiera comentar cuatro particularidades a tener en consideración respecto a los titulares de los datos en proyectos de big data (aplicados también a eHealth) que recoge el informe.

- En primer lugar, es de tener en cuenta que en los tratamientos convencionales de datos, la información acerca del tratamiento de sus datos se facilita al afectado en el momento de captación del dato, mientras que los tratamientos de *Big Data*, si por algo se caracterizan, es por su *continuidad en el tiempo.*

- En segundo lugar, los tratamientos de datos en entornos de *big data* se caracterizan también por la *combinación de las fuentes* (endógenas y exógenas). Y ello, no puede ser obstáculo para el ejercicio de derechos y se debe estar en posición de poder facilitar tanto el origen de la información como las comunicaciones de datos realizadas a terceros y, en su caso, las transferencias internacionales.

- En tercer lugar, las *disociaciones de los datos personales no deben ser una excusa* y una traba para cursar los derechos. Se debe estar en disposición de poder informar al afectado sobre el hecho de la anonimización, si se ha producido, y del riesgo de reidentificación existente en el caso del ejercicio de un derecho de acceso.

---

[895] Ídem, página 7.

[896] "Es un proceso que, mediante la aplicación del método científico de investigación, procura obtener información relevante y fidedigna (digna de fe y crédito), para entender, verificar, corregir o aplicar el conocimiento" . Vid. https://www.ecured.cu/Investigaci%C3%B3n_cient%C3%ADfica

[897] Si *innovación* es un cambio que introduce novedades y que se refiere a modificar elementos ya existentes con el fin de mejorarlos o renovarlos, podemos decir que innovación e investigación será la fusión de ciencia y tecnología respectivamente.

- En cuarto lugar, los encargados y responsables utilizarán *soluciones tecnológicas actuales y adecuadas*, que irán evolucionando con su desarrollo técnico.

5.4. Legitimación

5.4.1. El consentimiento.

La nueva era de la globalización y de las tecnologías disruptivas de salud ha propiciado inevitablemente sobreinformación de difíciles políticas de protección de datos en los entornos virtuales para los usuarios online. Un estudio de hace más de 10 años decía que una persona tardaría 244 horas o más de 30 días hábiles completos cada año (McDonald y Cranor, 2008)[898]. El advenimiento de Big Data y las nuevas herramientas analíticas nos han demostrado que muchos de los instrumentos valiosos y usos innovadores de los datos no se conocen en el momento de la recolección de los datos (Cullen y Mayer-Schönberger, 2014) [899]. En el sector de la salud, el *consentimiento* puede ser de *tiempo limitado* para que los datos no se usen cuando se haya expirado el tiempo límite máximo.

En definitiva, el nuevo paradigma del *consentimiento en proyectos de big data e investigación biomédica*[900] estaría marcado a mi modo de ver por las siguientes cuestiones:

i. *Un consentimiento dinámico.*

Nos encontramos en un momento de evolución del consentimiento; del sistema antiguo del "*consentimiento binario simple"*, el cual no se veía como compatible con el *análisis de big data* debido a su naturaleza experimental y a su tendencia a encontrar nuevos usos para los datos, al "*consentimiento graduado",* por el que las personas pueden dar su consentimiento o no, en

[898]. McDonald, A. y Cranor, L. (2008). El costo de leer las políticas de privacidad. *I / S: un diario de derecho y política para la informaciónSociety* Recuperado de http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Cranor_Formatted_Final.pdf

[899] Cate,F; Cullen, P. Mayer-Schönberger, V. (2014). Principios de protección de datos para el S. XXI. Revisión de las directrices de 1980 de la OCDE. *Universidad Oxford.* Recuperado de https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf

[900] Esto supondría un gran avance acorde al progreso tecnológico que estamos experimentando. Las grandes tecnológicas ya tienen acceso a datos masivos de salud a través de registros médicos que son analizados con el fin de mejorar el proceso *sin consentimiento* de los pacientes. Es el caso por ejemplo, de Google (*DeepMind*) [900] que tiene un acuerdo con el Sistema Nacional Público de Salud de Reino Unido en donde se analizan datos de pacientes con VIH positivas, abortos o sobredosis de los últimos cinco años, concretamente en 3 hospitales. El único fin es la asistencia sanitaria –y no la automatización de decisiones clínicas- y para oponerse al uso de sus datos deben contactar con el médico de cabecera. La IA de Google permitirá a los médicos hacer predicciones basadas en datos. New Scientist (2016). Vid. https://www.newscientist.com/article/2086454-revealed-google-ai-has-accessto-huge-haul-of-nhs-patient-data/.

función de los diferentes usos de sus datos a lo largo de su relación con un proveedor de servicios. El *informe*[901] del Comité Internacional de Bioética, (2017) propuso de manera reiterada a lo largo del mismo, el "consentimiento dinámico" basado en los principios de transparencia y participación, y que haría uso de la tecnología para superar los retos planteados por la propia tecnología el cual superaría al consentimiento amplio. El modelo se basaría en permitir a los usuarios controlar de forma permanente y dinámica qué uso se está haciendo de los datos, a través, por ejemplo, de portales de internet, y pudiendo consentir cada uso de dichos datos. No obstante, también surgen interrogantes acerco de cómo debería ser el uso y lo relativo a la neutralidad de la red y su acceso. Pensemos en sujetos fuente de países en vías de desarrollo. En todo caso se requeriría de la intervención de los poderes públicos en el control del proyecto y acciones de educación e información a los pacientes, algo más propicio de países desarrollados. En definitiva destaca la importancia de la actuación activa de los sujetos fuente, el liderazgo de los poderes públicos y la colaboración pública-privada para el uso legítimo y deseable de la "mina" de datos que se pueden generar.

ii. *El deber de información y la dificultad de determinar las finalidades.*

Respecto al deber de información (Art. 13 RGPD) para requerir el consentimiento, "cabe cuestionarse el grado de detalle posible al respecto de la misma en razón de la especial naturaleza y desarrollo del *big data*, *que hace bien difícil determinar las finalidades o comunicaciones* que van a producirse" (Cotino, 2017)[902]. Ya lo señalaba el SEPD (2015, 11)[903], "la transparencia y el control del usuario deben convertirse en realidad".

iii. *Particularidades de naturaleza técnica e innovación en la recogida del consentimiento.* Nos encontramos con la necesidad de que esta naturaleza técnica encaje adaptándose a las disposiciones del nuevo régimen jurídico de la mejor forma posible y siempre sin obstaculizar el progreso y desarrollo de la investigación biomédica. En el *informe* citado de (ENISA) se pidieron *más innovación técnica* -o automatización- en los métodos de obtener el consentimiento. Por ejemplo, los sensores y los dispositivos inteligentes se contabilizan en grandes datos, otros tipos de acciones positivas para el usuario utilizables y prácticas, que podrían constituir consentimiento (por ejemplo, gestos, patrones espaciales, patrones de comportamiento, movimientos), necesitan ser analizados" [904].

---

[901] *Supra Cit.*

[902] Cotino Hueso, L. (2017) . Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales. *Universidad de Valencia.* Nº 24, págs. 131-150.

[903] SEPD. Opinion 7/2015. Meeting the challenges of big data. A call for transparency, user control, data, protection by design and accountability. Recuperado de https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf

[904] D'Acquisito, Giuseppe et al. (2015). Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics. Pag. 46. *ENISA*, Recuperado de https://arxiv.org/ftp/arxiv/papers/1512/1512.06000.pdf

Y por último, respecto a la *reutilización de datos,* cabe señalar que la recopilación de datos personales masivos no solo requiere el consentimiento del interesado, sino que también que se limite la cantidad mínima (principio de minimización) de datos necesarios para lograr el propósito identificado y además que no se traten dichos datos para otros fines no relacionados sin un nuevo consentimiento.

5.4.2. Ejecución de contrato.

Por su naturaleza, la analítica de datos grandes, es probable que represente un nivel de análisis que va más allá de lo que se requiere a priori. Por lo que la mayor dificultad estará en demostrar que la analítica de *big data* es estrictamente necesaria para ejecutar un contrato.

5. 4.3. Misión de interés público.

El Reglamento prevé, algo que es relevante por cuanto nos interesa, y es que para determinadas finalidades, como pueden ser las relacionadas con un interés público esencial, las de investigación científica, las relacionadas con la atención sanitaria o social, o las relativas a salud pública, los tratamientos serán posibles en las condiciones que determine la legislación europea o nacional. Las normas correspondientes establecerán, además, las garantías necesarias para la protección de los derechos y libertades de los interesados[905].

El informe de la AEPD e ISMS, señalan que "normalmente, este tipo de tratamientos será llevado a cabo por entidades públicas, aunque sería posible identificar casos en que la atención de intereses públicos relevantes pudiera asumirse por entidades privadas. Ejemplos de tratamientos de Big Data, con o sin el empleo de datos personales, sobre esta base jurídica podrían ser los relacionados con proyectos de *Smart Cities* o los desarrollados por servicios públicos de salud".

5.4.4. Interés legítimo.

La condición de intereses legítimo no es una opción flexible (o cómoda) para el organización empresarial puesto que significa más responsabilidad, transparencia y

[905] El *HMRC Connect systeme*s es un ejemplo de análisis de big data en el sector público, basado en la condición por interés público o en el ejercicio de sus funciones, el cual utiliza más de un billón de datos de 30 fuentes para identificar posibles fraudes tributarios, incluyendo autodeclaraciones, intereses en cuentas bancarias, los beneficios y datos de créditos tributarios, mercados online y medios sociales, etc. Para más info: BDO. HMRC's evolution into the digital age. Implications for taxpayers. BDO, March 2015. http://www.bdo.co.uk/__data/assets/pdf_file/0011/1350101/BDO_HMRC_DIGITAL_AGE. pdf

compromiso[906][907]. El Dictamen 06/2014[908] menciona varios casos en los que dicho interés puede existir, tales como la libertad de información y expresión, las actividades de marketing o publicidad, prevención del fraude o mal uso de servicios, seguridad, finalidades científicas, estadísticas o de investigación. Para que sea considerado como base jurídica requiere que concurran estos requisitos: (i) "El responsable del tratamiento persigue un interés legítimo; (ii) El tratamiento de los datos personales es necesario para satisfacer el interés legítimo; (iii) Que no prevalezcan los derechos y libertades fundamentales del interesado por lo que se refiere a la protección de sus datos personales".

Y a los requisitos del *Dictamen 6/2014* hay que añadir la información de manera efectiva y transparente por el responsable del tratamiento al titular de los datos personales. Por ejemplo, si el proyecto consiste en un perfilado de marketing para mejorar un producto sanitario o la adherencia de un medicamento, actividad de la empresa o el método o la tecnología utilizado para el tratamiento de datos personales tiene que *ser necesario* para el interés legítimo del empleador y el tratamiento tiene que :

a. ser *necesario* y proporcional a las necesidades del negocio;
b. justificar que la tecnología *big data analítica es necesaria* para conseguir información y desarrollar la actividad empresarial;
c. se deberá llevar a cabo de la manera menos invasiva posible y estar dirigido al áreas específicas de riesgo, es decir, se dirigirá solo para un segmento de usuarios/ e-pacientes;
d. se deberá proporcionar información del derecho de oposición (art. 21 RGPD), del derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar (art. 22 RGPD), limitación del plazo de

[906] La ética tomará un papel muy importante donde ya empresas tecnológicas están creando comités de ética, esta cuestión la discutiremos más adelante. Para más info: http://www.europapress.es/portaltic/sector/noticia-sap-primera-tecnologica-europea-crear-grupo-asesor-etica-inteligencia-artificial-20180918182850.html

[907] Vid. Cullen, P.; Glasgow, J., Stan, C. (Octubre 2015) Introduction to the HGP framework. Information Accountability Foundation, pp. 29. Recuperado de http://informationaccountability.org/wp-content/uploads/HGP-Overview.pdf y http://informationaccountability.org/effective-data-protection-governance-project/. Así, la *Fundación por la Información Responsable* en un documento sobre un modelo de gobierno holístico para big data da ejemplos de los diferentes intereses en juego en IoT y sugiere que, si bien el consentimiento es importante para algunos usos de los datos, *para otros puede no ser apropiado*. Dada la complejidad asociada al consentimiento en un contexto de macrodatos, *el interés legítimo puede otorgar una solución viable para el procesamiento, permitiendo un equilibrio entre beneficios comerciales y sociales, y los derechos e intereses de individuos*

[908] Vid. Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE (WP 217)

conservación (Art. 5.1.e RGPD), derecho a supresión de datos (Art. 17 RGPD), y aplicando el principio de minimización de datos (Art. 5.1.c) , pseudonimización, etc.

5. 5. Decisiones individuales automatizadas.

En la Guía *de la AEPD-ISMS Fórum* (2017, 19), se señala acertadamente de tres aspectos regulatorios interesantes respecto de las decisiones automatizadas que tendrán una gran trascendencia en cualquier proyecto de Big Data, a destacar lo siguiente:

i. En primer lugar, "los principios de protección de datos, no deben aplicarse a la información anónima, (…), ni a los datos convertidos en anónimos de forma que el interesado a quien se refieren no sea, o ya no resulte, identificable. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, ni siquiera con fines estadísticos y de investigación" (considerando 26 del RGPD).

ii. En segundo lugar, "el RGPD da mucha importancia a los principios relativos al *tratamiento leal y transparente* de los datos, incluyendo la existencia de las elaboraciones de perfiles y de sus consecuencias. El artículo 22 del RGPD regula una variante del derecho de oposición respecto de las decisiones individuales automatizadas, incluida la elaboración de perfiles, que va a tener una gran importancia en los tratamientos de Big Data. Según el artículo 4.4 del RGPD, elaboración de perfiles es toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, ubicación o movimientos de dicha persona física. Por tanto es importante destacar que todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar".

   Ello supondrá que el interesado podrá oponerse a dicho tratamiento, pero siempre y cuando:

   a) la decisión "automatizada" o basada en *profiling* produzca efectos jurídicos que conciernan al interesado (v.gr. un seguro online que decide no otorgar póliza a una persona con ciertas dolencias) o;

   b) la decisión "automatizada" o basada en *profiling* le afecte significativamente.

   En este aspecto es importante tener en cuenta que la premisa básica es que exista una decisión *exclusivamente* "automatizada" sin que medie *intervención humana alguna*, debiendo informarse al interesado acerca de la existencia de un mecanismo de decisión automatizado que comprenda la elaboración de perfiles, la lógica aplicada, importancia y consecuencias para el interesado[909].

[909] En el *Dictamen del GT 29* sobre la toma de decisiones individuales automatizadas y la elaboración de perfiles (WP 251) resaltan las tres excepciones contempladas en el RGPD: (i)"Cuando la toma de decisiones automática es necesaria *celebración o la ejecución de un contrato*. Aquí, el GT29 reitera su opinión, ya publicada en su Dictamen sobre interés legítimo (WP217), de que la *«necesidad»* debe interpretarse en sentido estricto. Según el GT29, el responsable debe ser capaz de demostrar que la elaboración de perfiles es necesaria y que no se pueden adoptar métodos menos intrusivos para la

iii. En tercer lugar, "el último apartado del artículo 22 del RGPD establece una *prohibición general de adoptar decisiones individualizadas automatizadas* basadas en datos personales sensibles (origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos o datos relativos a la salud, vida y orientación sexuales) *salvo consentimiento explícito del interesado o por motivos de interés público, siempre que se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades, y los intereses legítimos del interesado".*

Podríamos decir que estos tratamientos están legitimados si existe; (i) el consentimiento expreso o por motivos de interés público; (ii) el derecho a obtener una intervención humana; (iii) el derecho a impugnar la decisión.

Ahora bien, algunas cuestiones que nos planteábamos en el capítulo 2[910], las retomamos ahora. En concreto, quisiera detenerme y compartir interrogantes que plantean autores[911] en la interpretación del art. 22 y la posible ampliación del alcance de la regulación de este precepto por los EEMM. Malgieri (2018), se pregunta si los legisladores nacionales podrán ampliar este alcance o si estarán permitidas las "decisiones positivas" o qué garantías podrán proteger mejor al individuo. Este autor llama la atención las iniciativas de EEMM como:

a) Francia y Hungría garantizan el *derecho a la legibilidad / explicación* de las decisiones algorítmicas.

b) Irlanda y Reino Unido *regulan la intervención humana* en la decisión algorítmica a través de un mecanismo efectivo de rendición de cuentas (por ejemplo, notificación, explicación de por qué no se ha aceptado tal impugnación, etc.).

c) Eslovenia requiere una *forma innovadora de evaluación de impacto* en los derechos humanos en la toma de decisiones automatizada.

En mi humilde opinión, se debería optar por llevar a cabo todas las máximas coberturas posibles para asegurar los derechos y libertades de las personas que van a ser sujetos de profiling o decisiones automatizadas; derecho a explicación, regulación de la

---

privacidad. Este requisito de necesidad aparentemente constituye un gran obstáculo para el responsable; (ii) Cuando esté *autorizada por ley* de un Estado miembro y (iii) cuando los interesados han dado su *consentimiento expreso*. El consentimiento expreso no está definido en el RGPD, pero se sugiere que debe estar basado en una acción afirmativa".

910 Se recomienda ver capítulo 2; "problemas de transparencia: elaboración de perfiles y decisiones automatizadas" (págs. 48-51) y ver ejemplos prácticos.

911 Malgieri, Gianclaudio. Automated Decision-Making in the EU Member States Laws: The Right to Explanation and Other 'Suitable Safeguards' (August 17, 2018). Recuperado de https://ssrn.com/abstract=3233611 o http://dx.doi.org/10.2139/ssrn.3233611

intervención humana, notificaciones y comunicación directa (y continua) con el sujeto, etc.

5. 6. Principios del RGPD aplicables. El papel de los desarrolladores.

5.6.1. Privacidad desde el diseño (Art. 25.1).

El proyecto *e-Health* de *big data* debe desarrollarse de tal manera que la privacidad se integre en las nuevas tecnologías y prácticas empresariales desde el momento cero. Se tratarán de medidas proactivas no reactivas y automáticas y serán consideradas como un componente esencial. Es conveniente saber que la privacidad por el diseño no es seguridad por el diseño, pero ambas están relacionadas. Además, se deberá aplicar a lo largo del ciclo de vida de los datos siendo visible y transparente. Es necesario pasar de la concepción de "big data versus privacidad" a "big data con privacidad" (D'Adquisto et al., 2015)[912].

5.6.2. Accountability o responsabilidad proactiva (art. 5.2. RGPD y 13.4 RGPD).

Cuando hablamos de este principio en proyectos de *big data* nos referimos a establecer procedimientos internos previos a la creación de operaciones de tratamiento; a establecer políticas escritas y vinculantes como la notificación o el acceso a datos, el nombramiento de un DPO; a la formación al personal, desarrolladores, etc.; a la existencia de un canal de quejas interno; a la realización de evaluaciones de impacto, a la existencia de mecanismos que apliquen y supervisen que las normas se cumplan. Es decir, "reconocer con toda diligencia; qué datos, para qué, por quiénes y cómo se tratan" (Ibáñez ,2018, 70).

En este último principio, quisiera detenerme para tratar su importancia en el labor desarrolladores. Un interesante y reciente estudio[913] donde ha participado la UC3M, analizó el software preinstalado en dispositivos Android y los riesgos para la privacidad de los usuarios. La investigación reveló la existencia de un complejo ecosistema de *fabricantes, operadores móviles, desarrolladores y proveedores de servicios*, donde m muchas de las apps preinstaladas facilitan el acceso privilegiado a datos y recursos del

[912] Cfr. D'Acquisto, G., Domingo-Ferrer, J., Kikiras, P, Torra, V., de Montjoye, Y., Bourka, A. (2015). Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics. *Cornell University*. Recuperado de https://arxiv.org/abs/1512.06000

[913] Gamba, J., Rashed, M., Razaghpanah, A., Tapiador J. ,Vallina-Rodriguez, N. An Analysis of Pre-installed Android Software. Recuperado de https://haystack.mobi/papers/preinstalledAndroidSW_preprint.pdf

sistema sin posibilidad de que un usuario medio pueda desinstalarlas. En este sentido, es de señalar el informe reciente que la AEPD ha publicado acerca de los "Análisis de flujos de información en Android. Herramientas para el cumplimiento de responsabilidad proactiva"[914].

5.7. Evaluaciones de impacto.

En el RGPD se exige la realización de evaluaciones de impacto como herramientas indispensables para evaluar "*el origen, naturaleza, particularidades y gravedad del riesgo,* en los casos en que las operaciones de tratamiento puedan dar lugar a un *alto riesgo para los derechos y libertades de las personas*". [915]Ahora bien, ¿cuándo debe someterse de forma obligatoria un proyecto de *big data* a una PIA?[916] El art. 35 RGPD establece que se deberá realizar evaluación de impacto cuando suponga un alto riesgo a los derechos y libertades de las personas físicas -con más razón en los *"profiling"* donde existan aspectos como la salud-. Un ejemplo puede ser una empresa de biotecnología como *Tellmegen*[917] que ofrece test genéticos a los consumidores para predecir riesgos de salud. Concretamente el RGPD, establece la necesidad de realizar la EIPD[918] siempre que se den las siguientes circunstancias;

---

[914] *Supra cit.*

[915] En el informe, los autores señalan a modo introductorio lo siguiente;"*Big Data* se caracteriza por incorporar en el *Business Intelligence o inteligencia empresarial* las fuentes de Internet (redes sociales, blogs, foros, medios de comunicación…), la actualización permanente de las mismas y el carácter continuo e inmediato de los análisis, hechos que exponen y elevan los riesgos potenciales para la privacidad. En este sentido, las organizaciones deben ser especialmente cautas con los *riesgos asociados a sus procesos de identificación, análisis y recolección de información.* Al adoptar nuevas soluciones tecnológicas como Big Data, todos los riesgos deben ser identificados y gestionados. Eso incluye desarrollar un *sistema de administración y gestión* de los mismos acorde con la estructura organizativa y los procesos relacionados con tratamientos de datos personales, que garantice la continuidad de los procesos, así como hacer frente, entre otros, a los riesgos legales y regulatorios.

[916] Vid. Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679. (WP 248).

[917] Vid. http://www.tellmegen.com/

[918] El contenido de la evaluación de impacto puede será (art.35 del RGPD): (i) *Descripción de los tratamientos*: tipo de datos (de salud), duración del tratamiento, tecnologías involucradas (big data) y sus aspectos funcionales, flujo de datos, destinatarios. Se deberá incluir el consentimiento al volumen de personas consultadas. (ii) *Valoración de riesgos*. Se detallarán los escenarios no deseados, amenazas, vulnerabilidades, consecuencias sobre las personas afectadas. Los impactos pueden resultar en pérdida de reputación, posibilidad de acciones sancionadoras o de responsabilidad. (iii) *Gestión de riesgos* evaluados y selección de medidas. Se deberá señalar hasta qué punto su influencia disminuye la probabilidad y sus consecuencias. (iv) *Análisis del cumplimiento normativo*. (v) *Informe final y conclusión*. Contendrá las recomendaciones (de eliminación, mitigación, transferencia o aceptación de los riesgos de privacidad). (vi) *Implantación de recomendaciones.* (vii) *Revisión y realimentación*. Se asignarán los recursos necesarios y se verificará el seguimiento de todas las fases del proceso. (viii) La organización debe establecer un *plan de supervisión y revisión* para auditar los resultados de la evaluación de impacto.

i. "Cuando las operaciones de tratamiento impliquen llevar a cabo una *evaluación sistemática y amplia de aspectos personales* relativos a personas físicas, que incluye la elaboración de perfiles, y especialmente si sobre el resultado del tratamiento se basan decisiones que produzcan efectos jurídicos sobre el individuo, o pueden afectar de manera significativa a los individuos.

ii. El *tratamiento a gran escala de datos sensibles*, es decir, los referidos en el artículo 9 del RGPD: los que revelen el origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona y datos relativos a la salud, la vida sexual o la orientación sexual de una persona.

iii. Los datos obtenidos del *control de áreas de acceso público a gran escala*, mediante monitorización por sistemas de video vigilancia".

5.8. Medidas necesarias.

Se conciben como *medidas obligatorias de obtener un resultado* (la no vulneración de los derechos de las personas), es decir, no se trata de una obligación de medios[919]. En este sentido la Sentencia de 11 de diciembre de 2008 de la Audiencia Nacional, (recurso 36/08)[920], señaló: "Como ha dicho esta Sala en múltiples sentencias…se impone, en consecuencia, una *obligación de resultado*, consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros[921]". Pero, ¿cuándo se impondrá una sanción por incumplir las medidas necesarias[922]? ¿cuándo será culpable el investigador o responsable del

[919] Cfr. Blanco Pérez-Rubio, L. (2014). Obligaciones de medios y obligaciones de resultado: ¿tiene relevancia jurídica su distinción? *Universidad Carlos III.* Recuperado de https://e-revistas.uc3m.es/index.php/CDT/article/viewFile/2260/1199

[920] Sentencia de Audiencia Nacional (Sala de lo Contencioso-Administrativo, Sección 1ª, de 26 de abril de 2012. Recuperado de http://cooperacionconcellos.deputacionlugo.org/portal_localweb/RecursosWeb/DOCUMENTOS/1/0_2578_1.pdf

[921] Así por ejemplo, en febrero de 2019, la Asociación de Usuarios de la Sanidad denuncia que el Servicio Murciano de Salud (SMS) no garantiza suficientemente la protección de los datos de los pacientes que piden cita por internet con su médico de familia o su enfermero de Atención Primaria. Declararon que "en este momento, cualquier persona que conozca la fecha de nacimiento y el DNI de otra podría acceder a los datos de los profesionales que le atienden y al número de su tarjeta sanitaria".

[922] La AEPD considera que el hospital "***no ha incorporado las medidas de seguridad adecuadas*** para impedir que desde el SERGAS se accediese a toda la información generada por el personal sanitario que presta servicios en el Centro Hospitalario con cargo a un aseguramiento privado". La AEPD ha declarado recientemente que "un hospital privado que da servicios al servicio de sanidad pública tiene que compartir los datos de los pacientes que vienen derivados de ella, **no así de los que acuden a sus instalaciones mediante aseguradora privada.** La información de estos pacientes ha de ser custodiada por el hospital, pero no compartida con los profesionales de la Sanidad Pública".
Vid. https://www.eprivacidad.es/multa-a-un-hospital-por-compartir-datos-procedentes-de-aseguradoras-privadas-con-el-servicio-de-salud-gallego/

tratamiento? La Sentencia del Tribunal Supremo de 27 de mayo de 1999 da una respuesta posible: "Para la imposición de una sanción y las consecuencias derivadas del ilícito administrativo, no basta que la infracción esté tipificada y sancionada sino que es necesario que se aprecie en el sujeto infractor el elemento o categoría denominado culpabilidad. La culpabilidad es el reproche que se hace a una persona, porque ésta debió haber actuado de modo distinto de cómo lo hizo". Por tanto, es necesario que se demuestre la culpabilidad.

En el procedimiento sancionador PS/00368/2015 R/02202/2015 de la AEPD encontramos un ejemplo práctico de culpabilidad. Se señaló que "en las normas para redactar los casos clínicos de este proyecto figura la advertencia: Se debe omitir toda referencia a datos personales identificativos de los enfermos o de sus familiares (nombres propios, lugares de residencia, etc.), así como cualquier información de los mismos que no sea relevante para el caso. Igualmente, se deben eliminar los nombres de hospitales e instituciones"[923]. En concreto, hablemos de las medidas técnicas y las medidas que generan confianza (u organizativas) que deberán salvaguardar el derecho fundamental de las personas.

5.8.1. Medidas técnicas.

Las diferentes técnicas o tecnologías que permitirían cubrir las diferentes estrategias de privacidad, según el informe de estas instituciones, podrían ser; "(i) la anonimización (serviría para las estrategias de minimizar o agregar); (ii) el cifrado (en el caso de ocultar o separar); (iii) el control de acceso (si se trata de informar o controlar); (iv) la trazabilidad (para las de cumplir o demostrar)". Pero hemos de añadir que se deben de tratar de "*medidas con obligación de resultado"* ya que el responsable será quien tenga especial diligencia en la custodia de la documentación o información de carácter personal.

5.8.2. Anonimización irreversible

Se recomienda seguir las recomendaciones del GT29 y de la AEPD, en concreto en su guía de anonimización se señalan las siguientes etapas o fases:

[923] Vid. https://www.laverdad.es/murcia/denuncian-cita-previa-20190214003636-ntvo.html

Tabla 50. Recomendaciones según fases del GT29 Y AEPD.

Al margen de definir un equipo de trabajo multidisciplinar, que definiría y planificaría el proceso de anonimización y los agentes implicados y sus funciones con un inventario funcional y orgánico, se requiere que se realice en un contexto de independencia profesional. Y en caso de que no fuera posible ésta se aconseja realizar un documento aprobado por el responsable de tratamiento donde conste los motivos y situaciones de las posibles segregaciones de funciones[924]. Hay que tener en cuenta que los procesos de anonimización tienen que adaptarse a los intereses legítimos de su destinatario y estará condicionado por su objetivo final, donde se podrán llevar a cabo acuerdos de confidencialidad y en el caso de información anonimizada de uso restringido se podrán valorar clausulas contractuales o códigos de conducta con el

[924] Visto lo anterior, y puesto que los procesos de anonimización tienen un impacto directo en los recursos de la organización (económico, tecnológico, humano) deberá ser adecuado. Algunos riesgos, por ejemplo, tienen que ver con la inadecuada gestión de claves o métodos basados en algoritmos de cifrado o huella digital y este riesgo aumentar a medida que transcurre el tiempo y existe más información sobre el propio interesado en las redes sociales, o blogs, por ejemplo. Se recomienda utilizar la guía (vid. https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf) para una evaluación de impacto en la protección de datos de la AEPD también y tener en cuenta algunas etapas como: (i) identificación y categorización de activos (grado de sensibilidad) como los propios datos personales, activos de información, hardware, software; (ii) constitución del equipo de trabajo; (iii) identificación de riesgos (conocidos, potenciales, no conocidos) por ejemplo, riesgos de vulneración del deber de secreto, la existencia de un atacante adversario potencial, etc.; (iv) valoración de riesgos o categorización; (v) salvaguardas para evitar los riesgos (en catalogo en función de la criticidad de los activos); (vi) cuantificación del impacto, por ejemplo, con diagramas con flujos de riesgos e imágenes gráficas de las zonas críticas con las salvaguardas, además hay que tener en cuenta que el impacto puede que ser tangible ¨(daños materiales, posibles indemnizaciones) o intangibles (pérdida de la confianza o deterioro de la imagen corporativa); (vii) informe de riesgos con carácter ejecutivo y se presentará al responsable del tratamiento y al equipo de seguridad para que emitan su dictamen; (viii) determinación del umbral de riesgos aceptable entre todos; (ix) gestión de los riesgos asumibles; (x) informe final con las medidas y conocido por todas las personas implicadas en los procesos; (xi) revisión de riesgos periódico a lo largo del ciclo de vida de la información y cuando se produzcan cambios.

compromiso por parte del destinatario de no realizar intento de reidentificación de personas que garantice esto incluso cuando se produzcan brechas de seguridad.
Además, por cuanto nos interesa, en la etapa 5ª, se podría valorar por parte del equipo un estudio de viabilidad del proceso de anonimización para categorías de datos especiales como son los de salud donde se incluyera, por ejemplo, vinculaciones éticas.
Llegados a la etapa 6ª de la pre-anonimización se tendrá en cuenta que las variables de identificación como son: los *identificadores directos* (o microdatos, que son las características que por sí mismas permiten la identificación de una persona) *o indirectos* (en combinación con otra información permiten la identificación como por ejemplo, el género, fechas como la de un ingreso hospitalario, etc.), *datos especialmente protegidos* (Art.9 RGPD), numéricos, temporales, metadatos (ver apartado de metadatos). En esta etapa se tendrá que tener en cuenta algo; las dificultades específicas de la anonimización para variables como por ejemplo, los datos genéticos, registros de voz o información biométrica.

A continuación, se reduciría al mínimo necesario la cantidad de variables que permitieran la identificación, y es que, a menos cantidad de datos personales, menor será el riesgo de reidentificación. Algunas cuestiones a tener en cuenta por ejemplo son; determinar la finalidad de los datos anonimizados como el uso científico o los plazos de conservación, establecer variables confidenciales necesarias para el tratamiento de los datos, eliminación e datos identificativos como son los nombres, fechas de nacimiento, email, teléfono, DNI, dirección IP, fotografía, etc.; o la utilización de rangos para "enmascarar" a las personas o contar con una política de claves para ocultar la identificación.

Respecto a la utilización de claves en el proceso de anonimización, la AEPD señala las siguientes técnicas; (i) algoritmos de hash; (ii) algoritmos de cifrado; (iii) sello de tiempo; (iv) capas de anonimización; (v) perturbación de datos; (vi) reducción de datos. Quisiera destacar la importancia, por un lado, de la técnica del sello del tiempo que garantiza la fecha y la hora en la que la anonimización han sido realizada y por otro lado, de las capas de anonimización, donde el legítimo destinatario asegura (con una segunda capa) con sus propios recursos de anonimización. Esta doble capa se pude utilizar atendiendo a la clasificación de las variables, de la organización interna o de garantías específicas de la política de anonimización.

Además de todo lo anterior, sería importante tener un mapa de sistemas de información que garantizara entornos separados para cada tratamiento de datos

personales, es decir, en un entorno segregado. Y por último, se recomienda un proyecto piloto que cuente con una pequeña muestra de datos de prueba no reales donde se pueda materializar la viabilidad de las propuestas de los miembros del equipo, y a continuación, se realizaría la fase de anonimización (determinando las técnicas más apropiadas, planificando las tareas de cada miembro del equipo, determinando los recursos validando la técnica por expertos como son los estadísticos o profesionales de la ética, ruptura relacional de las claves, recodificación, reducción de datos, revisiones, auditorías, etc.

No quisiera terminar este apartado sin destacar otros dos elementos esenciales; la formación de los miembros que intervienen y ejemplos de garantías en el proceso. Respecto a lo primero, nos referimos sobre todo a formación en lo relativo a las medidas del art. 32 RGPD. El personal será informado de la existencia y aplicación de la política de anonimización (principios de protección de datos, objetivos EIPD, objetivos y finalidad de la información anonimizada, variables, técnicas), términos de uso y acceso a la información anonimizada, medidas de control, y obligaciones y deberes. Además, no olvidemos que en la LOPDGDD (art. 2 apartado p) se regula como muy grave "la reversión deliberada de un procedimiento de anonimización a fin de permitir la reidentificación de los afectados"[925].

Por otro lado, como establece la AEPD e ISMS (2017, 30),"aunque los procesos de anonimización y disociación son clave para respetar la privacidad en los análisis de Big Data, no hay que desdeñar *otras medidas técnicas* aplicables al desarrollo de cualquier sistema, aunque con particularidades propias para su aplicación a Big Data[926]. Y a su vez, estas técnicas podrían estar contenidas en las siguientes implementaciones en función de la fase de *big data* en la que el proyecto empresarial se encuentre:

Fase Big Data	*Estrategia*	*Implementación*
Adquisición y recolección	Minimizar	Seleccionar antes de adquirir
	Agregar	EIPD
	Ocultar	Anonimización en la fuente origen
	Informar	Transparencia-comunicación del interesado
	Controlar	Mecanismos para recabar consentimiento
Análisis y validación	Agregar	Técnicas de anonimización
	Ocultar	Herramientas de cifrado

[925] Un procedimiento sancionador es lo que perseguían la NHS inglés, por ejemplo.
[926] CSA (2013). Expanded Top Ten Big Data Security and Privacy Challenges. Recuperado de https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Expanded_Top_Ten_Big_Data_Security_and_Privacy_Challenges.pdf

Almacenamiento	Ocultar Separar	Herramientas de cifrado Mecanismos de autenticación y control de acceso. Almacenamiento distribuido/descentralizado
Explotación	Agregar	Técnicas de anonimización
Todas las fases	Cumplir/demostrar	Definición de políticas Trazabilidad de las acciones Herramientas de cumplimiento

Tabla 51. Fases y Códigos de buenas prácticas en protección de datos para proyectos *Big Data*. Pag. 29[927]

5.8.3. Medidas que generan confianza.

En primer lugar, las organizaciones tienen que tener en cuenta de no recoger datos excesivos para esa finalidad (principio de minimización). El hecho de que se puedan recoger para finalidades diferentes en el futuro, no significa que se recojan "*por si acaso"*. No obstante, si en el momento en el que nos planteamos qué campos anonimizar, optamos por la *anonimización del conjunto completo* de los datos de salud, esto "podría derivar en una pérdida de información relevante a la hora de extraer conocimiento de los datos recogidos de los pacientes" (Lozoya de Diego et al., 2016, 294)[928] y como hemos dicho en párrafos anteriores, poner el peligro el desarrollo de la investigación biomédica en entornos de big data. Por tanto, como señalan los autores, "es necesario realizar una correcta elección de los datos que deben ser anonimizados, de manera que se pueda extraer conocimiento de los mismos garantizando el derecho a la protección de datos del paciente" (extendiendo la categoría de paciente a usuario o consumidor de eHealth). Posiblemente tal y como señala el código de buenas prácticas, el "principio de minimización puede ser el más relevante en el entorno de la tecnología de *big data*"

En segundo lugar y desde una perspectiva general, no podemos pasar por alto la mención expresa que realiza el legislador con el *"principio de seguridad de la información"* en el que se tiene en cuenta particularmente los riesgos asociados a la destrucción, pérdida o alteración, o comunicación o acceso no autorizado. Ni tampoco,

[927] *Supra cit.*
[928] Lozoya de Diego, A.,Villalba de Benito, M.T., Arias Pau, M. (2017). Taxonomía de información personal de salud para garantizar la privacidad de los individuos". El profesional de la información. marzo-abril, V.26, N.2. Recuperado de http://www.elprofesionaldelainformacion.com/contenidos/2017/mar/16.pdf

la importancia y la necesidad de extremar las medidas para aquellos datos de salud que operen en entornos de *cloud computing* y *big data*[929].

En tercer lugar, este tipo de proyectos se podrán valer de las herramientas que pone el legislador a nuestra disposición como son los citados en este capítulo, *códigos de conducta, mecanismos de certificación, sellos o etiquetas* de protección de datos (Art. 40 a 43 RGPD). Respecto a los códigos de conducta, tal y como se señala en el informe, se espera que próximamente salgan a la luz nuevos códigos de conducta referentes al procesamiento masivo de datos que ayuden a las organizaciones a aplicar la nueva regulación de forma adecuada. Y respecto a las certificaciones aplicables para proyectos de big data, en el informe se señala como la más conocida a *EuroPriSe*, que ofrece certificaciones para productos y servicios IT que cumplen con la legislación europea de protección de datos.

5.9. Buenas prácticas.

Existe un factor del que no nos podemos desentender y es la continua evolución tecnológica y esto conlleva, como señalan en el informe, a que "los procesos realizados no sean definitivos o irreversibles, ya que dependerán del avance de la técnica y de las fuentes de datos conocidas". Por ello, la solución estará en tomar decisiones caso por caso y optar por combinar técnicas que eviten principalmente la identificación (o "re-identificación") del titular de los datos sobre todo al usar varias fuentes de información, sean o no accesibles al público. Para ello, la AEPD y el ISMS han señalado como buenas prácticas entre otras las siguientes:

i. La protección de datos desde el diseño ("*privacy by design*") como centro de actuación impulsando los análisis de impacto.
ii. La valoración del uso de la anonimización en relación con sus *requisitos previos o contexto* y la finalidad del proceso de anonimización que buscamos, antes de aplicarla.
iii. La *revisión* periódica de la anonimización (riesgos residuales, nuevas fuentes, nuevas tecnologías).
iv. La observación y preservación de la *utilidad de los datos* en las técnicas de anonimización en la medida de lo posible, sin perder de vista el impacto que puede tener la utilización de las mismas, especialmente en el caso de elaboración de perfiles.

[929] Como vimos en el capítulo 2, la particularidad de este sector hace que las tecnologías puedan ser utilizadas de manera complementaria. El tratamiento masivo de datos requiere de infraestructuras de almacenamiento capaces de albergar dicha información.

v. La *distinción* entre "seudonimización y anonimización" de la que ya hemos hablado en este capítulo.

vi. El establecimiento de medidas adicionales de seguridad como son las *auditorías periódicas* de las fuentes de información, *de los canales de transmisión* de la información, *de las localizaciones físicas* de las fuentes de información, etc., También se tendría que tener en cuenta protocolo posible de notificación de brechas de privacidad en casos de re-identificación.

vii. El desarrollo de códigos de conducta, la aplicación de estándares, sellos y buenas prácticas en seguridad y privacidad de la información.

5.10. Retos y desafíos

i. La importancia de la anonimización (irreversible) en la investigación biomédica.

La Guía de la AEPD sobre "Orientaciones y garantías en los procedimientos de anonimización de datos personales"[930] no permite albergar grandes esperanzas sobre esta técnica y así lo deja esclarecer;

> "No es posible considerar que los procesos de anonimización garanticen al 100% la no reidentificación de las personas, por lo que será necesario sustentar la fortaleza de la anonimización en medidas de evaluación de impacto (EIPD), organizativas, de seguridad de la información, tecnológicas y, en definitiva, cualquier medida que sirva tanto para atenuar los riesgos de reidentificación de las personas como para paliar las consecuencias de que éstos se materialicen"

La AEPD considera que el desarrollo de técnicas de anonimización de datos adquiere una "importancia vital" para garantizar la protección de datos personales en el desarrollo de estudios e investigaciones de interés científico donde están embebidas se las investigaciones biomédicas. La anonimización de los datos personales adquiere un valor especial como fórmula que posibilita garantizar el avance de la investigación (y de la sociedad, por ende) sin menoscabar el respeto al derecho fundamental de la protección de datos.

La necesidad de *garantizar la irreversibilidad de la anonimización* es evidente y está más que asimilada. El avance de la tecnología y los grandes volúmenes de información disponibles hacen difícil garantizar el "*anonimato absoluto*". En este sentido, la AEPD aconseja entre otras medidas, técnicas que requieran un *coste lo suficientemente alto que la "reidentificación" resulte ser inviable o inasumible en*

[930] AEPD. Orientaciones y garantías en los procedimientos de Anonimización de datos personales. Recuperado de https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf. Pto. 8

términos de "esfuerzo-beneficio". Por tanto, como se puede intuir será necesario, por un lado, *valorar los riesgos* de esa *reidentificación* (tarea nada baladí) y por el otro, tomar y elegir *medidas organizativas* (como la definición de un equipo de trabajo[931], la formación del personal, las medidas de confidencialidad, el uso de posibles estándares, la utilización de códigos de buenas prácticas, etc.). Todo ello se convertirán en "instrumentos de evidencia" de cumplimiento normativo y de diligencia por parte del responsable.

Pero no resultará nada sencillo. La AEPD ya ha señalado en su guía que "el rápido avance tecnológico podría dejar obsoletas las técnicas de anonimización elegidas en un corto espacio temporal con la aparición de técnicas más seguras o la aparición de técnicas que permitan vulnerarlas". Pero no sólo eso, sino que la adopción de varias técnicas tendrá que estar supeditado a la valoración de las técnicas en el ámbito de la investigación donde se necesitará, a mi modo de ver, varias fases de análisis, de cuantificación y valoración de los riesgos teniendo en cuenta las capacidades de terceros en realizar reidentificaciones, y optando por medidas como cláusulas contractuales con penalización, etc. en caso de que sea posible, o en otros casos, utilizar la tecnología para minimizar dichos riesgos.

Por ejemplo, pensemos en los perfiles genéticos donde si se utiliza únicamente la técnica de eliminación de la identidad del donante. Según el abogado Álvarez[932], "diversos estudios científicos han demostrado que, al combinar los recursos genéticos disponibles para el público (p. ej., registros genealógicos, obituarios y resultados de consultas en motores de búsqueda) y los metadatos sobre donantes de ADN (fecha de donación, edad o lugar de residencia), se puede revelar la identidad de determinadas personas aunque el ADN se haya donado de forma anónima".

---

[931] Llama la atención como la AEPD señala algunos de los perfiles que participarían en el proceso de anomimización como son el DPD, responsables, destinatario, equipo de evaluación de riesgos, equipo de preanonimización y equipo de anonimización, equipo de seguridad de la información y del proceso de anonimización, responsable de seguridad y resto del personal involucrado en tareas de seguridad de la información (operadores de seguridad, responsables de seguridad de la información departamentales o de zona, responsables de sistemas de información, etc.), comité ético, etc. Esto se traduce en la intervencion de múltiples actores y múltiples tareas dentro del proceso. Aunque, "la disponibilidad de personal y recursos que ello exige resulta sencillamente inalcanzable para la investigación básica en la mayoría de las universidades de este país y me atrevería a decir que en gran parte de los hospitales y sistemas de salud (MARTINEZ, 2017, 274).

[932] Álvarez Hazas, G.Anonimización de datos personales de la investigación. Perspectiva jurídica y práctica. Mallorca, 2018. Recuperado de https://gahazas.files.wordpress.com/2018/11/anonimizacic3b3n-de-datos-personales-para-investigacic3b3n_v3.pdf

Surgen en este ámbito varios interrogantes; ¿qué preocupa más el hecho de tratarse de tratamiento de datos personales de categoría especial o que estos sean identificables en el ámbito de la investigación biomédica? ¿sería igual de susceptible de *infracción* (Art. 72.p LOPDGDD) aquellos hechos donde hayan existido dolo y voluntariedad respecto de aquellos que no hubiera existido intención por parte de los responsables de tratamiento o de los investigadores y se presuma buena fe? ¿Cuándo será imprudencia por parte de éstos últimos? Encontramos la respuesta en el procedimiento sancionador PS/00368/2015 R/02202/2015 de la AEPD, cuando señala: "El Tribunal Supremo viene entendiendo que existe imprudencia *siempre que se desatiende un deber legal de cuidado*, es decir, cuando el sujeto infractor no se comporta con la diligencia exigible. Diligencia cuyo grado de exigencia se determinará en atención a las circunstancias concurrentes, tales como el especial valor del bien jurídico protegido, la profesionalidad exigible al infractor. En este sentido la Sentencia de 5 de junio de 1998 exige a los profesionales del sector... *un deber de conocer especialmente las normas aplicables*".

ii. El principio de finalidad y proporcionalidad de las medidas.

Las investigaciones biomédicas en entornos de *big data* y *machine learning,* se extrae información procedente de los historiales clínicos (como fuente de información). Ahora bien, determinar la finalidad es totalmente necesario para desarrollar el *juicio de proporcionalidad*[933] que se exige para cumplir la normativa.

Imaginemos una investigación biomédica (con base legítima del consentimiento expreso) sobre enfermedades cardiorespiratorias en la que se identifican patrones de riesgo y producen efectos neurológicos para el paciente.

El profesor Martínez es bastante contundente en este sentido (2017, 259)[934]: "… salvo que las autoridades de protección de datos admitan que la investigación científica en salud constituye por sí misma un supuesto de interés legítimo, Big data no será viable en la Unión Europea".

[933] Como señala el SEPD en las Directrices sobre la proporcionalidad (2019), Véase TJUE, asuntos acumulados C-465/00, C-138/01 y C-139/01, Rechnungshof, ECLI:EU:C:2003:294, para. 52: "El Gobierno austriaco señala, en particular, que, al revisar la proporcionalidad, debe tenerse en cuenta hasta qué punto los datos afectan a la vida privada. Por lo tanto, los datos relativos a la intimidad personal, *la salud,* la vida familiar o la sexualidad *deben protegerse más* que los datos relativos a la renta y los impuestos, que, aunque también son personales, se refieren en menor medida a la identidad personal y, por lo tanto, son menos sensibles".

[934] *Supra cit.*

Ahora bien, acudamos al marco normativo y a la interpretación de la AEPD. Si acudimos al RGPD para dar respuesta, encontraremos el Considerando 50 que señala; "las operaciones de tratamiento *ulterior* con fines de archivo en interés público, fines de *investigación científica* e histórica o fines estadísticos deben considerarse operaciones de tratamiento lícitas compatibles". *No existe duda con este considerando la intención del legislador respecto a las operaciones de tratamientos ulteriores y su licitud. No cabe duda que el legislador europeo pretende facilitar y desprenderse de posibles barreras en el campo de la investigación biomédica y su desarrollo.* No obstante, de este considerando se pasó una interpretación más restrictiva con el considerando 33, es consciente de la problemática que se produce en este ámbito y en pro de los derechos de los interesados se exige que éstos tengan la oportunidad de darlo sólo para determinadas áreas o proyectos de investigación:

> "Con frecuencia *no es posible determinar totalmente la finalidad* del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida. Por consiguiente, debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para la investigación científica. Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida"

Llegados a este punto, una interpretación por parte de las autoridades nacionales es importante. En 2018, la AEPD en su *informe acerca de la incidencia que en el ámbito de la investigación biomédica y la plena aplicación del RG*PD[935] dio su parecer estableciendo que tomando a la base jurídica como la investigación biomédica y la legislación sanitaria, no se interpretará de modo restrictivo, limitado a una concreta investigación. Estableció concretamente que; "será suficientemente inequívoco y específico el consentimiento prestado en relación con una rama amplia de investigación, como por ejemplo, la investigación oncológica, o *incluso para ámbitos más extensos*".

¿Podríamos entender que la expresión "ámbito más extensos" incluye tratamiento de datos en el campo de la investigación de diferentes enfermedades (cardiorespiratorias y alzhéimer) con componentes de conexión entre sí y tratarse de un tratamiento de datos legítimo?

[935] *Supra cit.*

Visto todo ello, nos encontramos con un escenario con diferentes interpretaciones acerca de la cuestión.

La visión del profesor Martínez (2017, 260) me parece acertada:

> "En primer lugar, salvo habilitación legal expresa, -que recordemos tardará de dos a tres años en llegar-, los operadores en Sanidad deberían cuidarse mucho de obtener el consentimiento libre, específico, informado e inequívoco por el que el interesado acepta de modo explícito, ya sea mediante una declaración o una clara acción afirmativa, el uso de sus datos con fines de investigación en salud. *Ello implicaría en una interpretación estricta identificar el área concreta de investigación en salud*".

Este autor no aconseja que investigadores o responsables del tratamiento opten como base legitimadora el consentimiento del paciente puesto que implicaría la interpretación estricta parcelando un área concreta de investigación, por ejemplo, alzhéimer o enfermedades cardiovasculares.

> "Un segundo escenario, consistiría bien en entender que consentir para la «investigación en salud» es suficientemente específico, o bien considerar que el uso posterior de los datos para «otros fines de investigación en salud» no es incompatible. De no manejar este tipo de criterios resultaría una paradoja singular. Si aplicamos el principio de finalidad en sentido estricto, resultaría que tal vez hubiéramos descartado el Sindenafil como principio activo adecuado para tratar la angina de pecho y jamás habríamos contribuido a remediar la disfunción eréctil «por protección de datos».

Desde mi humilde punto de vista y dando la razón a este segundo punto de reflexión del profesor y a la queja colectiva de la comunidad científica de la que hemos hecho eco (previa la entrada en vigor de la LOPDGDD), el encaje de una interpretación cerrada puede derivar en un retroceso en la evolución y desarrollo científico.

La Sociedad Española de Cirugía y Traumatología (SECOT)[936] es un ejemplo de comunidad científica que investiga, que fue sancionada hace unos años (R/02202/2015, PS/00368/2015) por haber dejado una imagen de una parte del cuerpo de un paciente con datos identificativos accesibles por el visor de casos clínicos para residentes.

[936] https://www.secot.es/visor/index.php

Imagen 71. Pantallazo Secor. Fuente: Secor

5.11. Una aproximación a las posibles soluciones

i. *Ética organizacional o institucional y principio de responsabilidad proactiva.* Los valores de la confidencialidad, la privacidad y su protección son imprescindibles y están presentes en la actualidad como valores a asegurar en el marco de las organizaciones privadas y las instituciones públicas. Lo mismo sucede con la responsabilidad proactiva en materia de privacidad y protección de datos y sus medidas de las que hemos hablado a lo largo del capítulo. Posibilitar y garantizar un buen nivel transparencia entre investigadores y responsables del tratamiento y pacientes es imprescindible, y en este sentido, puede ser recomendable en pro del derecho fundamental de los pacientes determinar el consentimiento como base jurídica del tratamiento de datos (y no el interés legítimo o ejercicio de poderes públicos). La actitud preventiva es importante, por ello, se recomienda disponer políticas preventivas de análisis de riesgo y delimitar la finalidad de la investigación (tal y como hemos hablado en el punto anterior) incluyendo estrategias en la formación ética de los equipos de investigación. Y por último, a ser posible, se recomendaría evitar contexto donde se produzcan decisiones automatizadas.

ii. *Gobernanibilidad: Proceso de anonimización con sus fases.* Se recomienda seguir las recomendaciones del GT29 y de la AEPD que hemos mencionado en el apartado anterior.

iii. *Concienciación sobre el valor y las liberaciones de datos.* El NHS (Sistema de sanidad ingles) trata a aproximadamente un millón de personas cada 36 horas, y recopila una gran cantidad de información sobre cómo han sido tratados los pacientes y cuáles han sido sus resultados. En este momento, esta información se mantiene por separado en todo el NHS[937]. Según el estudio inglés

[937] Vid. https://www.england.nhs.uk/2013/10/care-data/

de *Welcome Trust*[938](2013), acerca de la preocupación de los encuestados por la pérdida del anonimato o el extravío en "manos equivocadas" de los datos de salud en el marco de los ensayos clínicos o investigaciones biomédicas fue de nivel bajo. Se comprobó que aquellas personas que fueron informadas de que los datos de salud tenían un "valor" (económico o social) respaldaban (con más probabilidad) a su acceso que los que no[939].

6. PARTICULARIDADES JURIDICAS DE LAS ASEGURADORAS DE SALUD Y PROTECCIÓN DE DATOS A TENER EN CUENTA.

La industria aseguradora no avanza ni se transforma puesto que lleva siglos vendiendo, no obstante, algo está cambiando con la digitalización. Las aseguradoras integran ya el chat médico de 24 horas para enviar fotos, videos, analíticas, pruebas, etc. y permiten el contacto con el profesional sanitario a través de videoconferencia (Sanitas). También están invirtiendo en el análisis de grandes volúmenes de datos o *big data* para la toma de decisiones y estudiar nuevos productos y servicios. La tecnología les posibilita contar con información para *lograr predicciones estadísticas* sobre el comportamiento de los asegurados, mejorando y personalizando las ofertas de las

[938] Welcome. Ac.Uk. Datos de paciente en investigación. Recuperado de https://wellcome.ac.uk/what-we-do/our-work/our-policy-work-using-patient-data-research

[939] Welcome. Ac.Uk. Ensuring the effective use of patient data. Recuperado de https://wellcome.ac.uk/sites/default/files/ensuring-the-effective-use-of-patient-data-briefing-aug15.pdf. En ese estudio los encuestados "donarían" sus datos: a. Si tienen el *control de los datos*. Es decir, controlar qué datos se comparten, quiénes tiene acceso a los datos, para qué se utilizarán los datos y quién se beneficiará de tal uso. Algunos de los entrevistados señaló que antes de cualquier uso de los datos, el permiso debe solicitarse al propietario. b. Si existe *transparencia* y comunicación en todo el ciclo de la información. La falta de comunicación puede poner en riesgo su confianza y con ello, la participación de los miembros. c. Si conserven el *anonimato* (datos estén anonimizados) y seguridad. En concreto se refieren a la re-identificación de la que venimos hablando. En varias respuestas se sugirió que se deben aplicar diferentes procedimientos en función de sobre la probabilidad de ésta. Además, "los sistemas de almacenamiento deben ser lo suficientemente robustos como par para soportar ataques informáticos, que son cada vez más frecuentes en el sector de la salud"[939]. d. Si se trata de un *beneficio colectivo y de la sociedad* (más que de un sistema de compensación económica). "Los encuestados creen que un sistema compensación económica la a los individuos que deciden dar sus datos puede tener un efecto negativo. Ellos señalaron que la sangre y modelos de donación de órganos como buenos ejemplos, ya que en ellos el *altruismo* prevalece sobre cualquier beneficio individual para la comunidad". Por tanto, consideran que la venta de datos no tendría efectos positivos. En el estudio, destacan tres aspectos importantes en relación con la promoción de investigación biomédica para el bien común: "(i) la importancia de fomentar el acceso abierto a publicaciones de investigación; (ii) la importancia de publicar todos los resultados de ensayos clínicos; (iii) investigación libre y responsable que se dirige a las necesidades reales de la sociedad". Existe un claro riesgo para la mayoría de los encuestados en relación con los *datos que se utilizan con fines de lucro*, que no beneficiaría a los ciudadanos e incluso podría utilizarse contra de ellos. Por ejemplo, el caso más destacado tiene que ver con el *seguro de salud,* del que hablaremos a continuación.Si se garantiza el *uso eficaz* de los datos de los pacientes necesario para mejorar la prestación de la asistencia sanitaria, diseño de servicios e investigación médica en el NHS.

aseguradoras. Al fin y al cabo, "las Compañías de seguros tienen un interés justificado en la distribución simétrica de la información, ya que si no se da una distribución simétrica de la información, puede que se produzca una pérdida actuarial, que a la larga podría poner en peligro la viabilidad de la Compañía de seguros" (HERRERA, 2010,61).

Al margen de la economía del mercado y de los intereses comerciales de las organizaciones de este sector, éstas deberán estar al tanto y cumplir la normativa correspondiente en materia de protección de datos, tanto los posibles cedentes (proveedores de salud, empresas tecnológicas, etc.) como los posibles cesionarios (por ejemplo, aseguradoras). En este sentido, "la Audiencia Nacional, en varias sentencias, entre otras las de fechas 14 de febrero y 20 de septiembre de 2002 y 13 de abril de 2005, exige a las entidades que operan en el mercado de datos una *especial diligencia a la hora de llevar a cabo el uso o tratamiento de tales datos o su cesión a terceros*" (PS/00368/2015 R/02202/2015)

6.1. Finalidades del tratamiento de las aseguradoras.

Desde el Consejo de Europa en el 2016 ya se hizo pública una recomendación referente a los datos de carácter personal relativos a la salud. En la cual señalaban que *sólo* deberían tratarse con fines de seguros sujetas a las siguientes condiciones (principio 1): (i) si el propósito de procesamiento se especificaba y la relevancia de los datos era *debidamente justificada*; (ii) si la calidad y validez de los datos están en conformidad con los estándares científicos y clínicos generalmente aceptados; (iii) si los datos resultantes de un examen predictivo tienen un *alto valor predictivo positivo*; (iv) si el tratamiento está debidamente justificado de conformidad con el *principio de proporcionalidad* en relación con la naturaleza y la importancia del riesgo de que se trate.

6.2. Legitimación

La Disposición adicional decimoséptima de tratamiento de datos de salud de la LOPDGDD, señala que;.

> 1. Se encuentran amparados en las letras g), h), i) y j) del artículo 9.2 del Reglamento (UE) 2016/679 los tratamientos de datos relacionados con la salud y de datos genéticos que estén regulados en las siguientes leyes y sus disposiciones de desarrollo:

(…) h) La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

Esto quiere decir que la prohibición que se mantenía para los datos de categoría especial podrá ser eximida (cuando el tratamiento es necesario por razones de un interés público esencial (9.2.g); para fines de medicina preventiva o laboral (9.2.h); por razones de interés público en el ámbito de la salud pública (9.2.i); con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos (9.2.j); para los tratamientos de datos que estén regulados en la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras[940] (entre otras que señala el legislador nacional).

Por su parte, el art. 99 de esa ley sectorial indica que:

"1. Las entidades aseguradoras podrán tratar los datos de los tomadores, asegurados, beneficiarios o terceros perjudicados, así como de sus derechohabientes *sin necesidad de contar con su consentimiento* a los solos efectos de garantizar el pleno desenvolvimiento del contrato de seguro y el cumplimiento de las obligaciones establecidas en esta Ley y en sus disposiciones de desarrollo. El tratamiento de los datos de las personas antes indicadas para cualquier finalidad distinta de las especificadas en el párrafo anterior deberá contar con el consentimiento específico de los interesados."

O dicho con otras palabras, la base legitimadora del tratamiento de los datos personales no se sustentaría en el consentimiento sino en la ejecución de un contrato (Art. 6.1. b RGPD) y el cumplimiento de obligación legal (art. 6.1.c RGPD). Pero además, consiente el tratamiento para la determinación de asistencia y la indemnización o para el abono a los prestadores sanitarios[941].

[940] Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras. Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-2015-7897

[941] "2. Las entidades aseguradoras podrán tratar sin consentimiento del interesado los *datos relacionados con su salud* en los siguientes supuestos: a) Para la determinación de la asistencia sanitaria que hubiera debido facilitarse al perjudicado, así como la *indemnización* que en su caso procediera, cuando las mismas hayan de ser satisfechas por la entidad. b) Para el adecuado abono a los prestadores sanitarios o el reintegro al asegurado o sus beneficiarios de los gastos de asistencia sanitaria que se hubieran llevado a cabo en el ámbito de un contrato de seguro de asistencia sanitaria. 3.El tratamiento de los datos se limitará en estos casos a aquellos que resulten imprescindibles para el abono de la indemnización o la prestación derivada del contrato de seguro. Los *datos no podrán ser objeto de tratamiento para ninguna otra finalidad*, sin perjuicio de las obligaciones de información establecidas en esta Ley".
En estos aptdo. 2 y 3, parece hacer referencia a la base legal del tratamiento de datos esté en la ejecución de un contrato (Art. 6.1. b y art. 9 RGPD). Tiene su lógica, pero veremos más adelante que hay que evitar accesos a historiales clínicas alegando esta justificación cuando ésta no sea la real.

6.3. Cesión de datos personales[942] con finalidad de "selección de riesgos".

La selección de riesgo médica, "consiste en analizar las diversas afecciones que vengan descritas en los cuestionarios de salud de los candidatos, y en función de una serie de reglas, conocimientos y experiencia, poder descartar al candidato que no se ajuste al perfil que la compañía desee o acotar coberturas" (Herrera, 2010, 34)[943]. Existen factores como la edad, género, estado de salud, lugar de residencia, profesión, estilo de vida, aficiones y hábitos…etc.

En el aptdo. 7 de del art. 99 llama la atención la referencia de los ficheros comunes con finalidad de "selección de riesgos" entre otras cuestiones.

> "7. Las entidades aseguradoras podrán establecer ficheros comunes que contengan datos de carácter personal para la liquidación de siniestros y *la colaboración estadístico actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora*. La cesión de los citados datos no requerirá el consentimiento previo del afectado, pero sí la comunicación a éste de la posible cesión de sus datos personales a ficheros comunes para los fines señalados, con expresa indicación del responsable, para que se puedan ejercitar los derechos de acceso, rectificación, cancelación y oposición previstos en la ley.
>
> (…) En todo caso, los datos relativos a la salud sólo podrán ser objeto de tratamiento con el consentimiento expreso del afectado".

6.4. Recogida de datos personales de salud

6.4.1. Calidad de los datos.

La información puede ser recogida a través de los documentos de solicitud de salud o los cuestionarios con preguntas de ámbito de salud (amplio, reducido o mixto)[944]. ¿Qué ocurriría si las aseguradoras pretendieran acceder a la información personal médica de los historiales médicos como justificantes médicos de facturación para el abono por determinada asistencia sanitaria prestada? Todo aquello que se

---

[943] Herrera Ruíz, F.J. (2010). *Selección de riesgo en el Seguro de Salud. Seguros de Asistencia Sanitaria.* (Trabajo fin de Máster, Universidad de Barcelona). Recuperado de http://www.servidor-gestisqs.com/ub/intranet/pdf/tesis_alumnos/Javier_Herrera.Seleccion_Salud.pdf

[944] El cuestionario mixto por ejemplo detalla antecedentes personales, familiares, patológicos, y todos aquellos datos que pueden ser de interés para la Compañía aseguradora. Las preguntas realizadas al asegurado deberán ser adecuadas, pertinentes y no excesivas en relación con el ámbito y la finalidad perseguida, tal y como establece el artículo 5.1.c ("principio de minimización") y 5.1.b. del RGPD ("limitación de la finalidad"). De esta forma, las preguntas contenidas en el cuestionario o (del reconocimiento médico) tendrían que ser únicamente los estrictamente adecuados y pertinentes para la finalidad concreta y determinada que se pretenda perseguir. Además, en la Recomendación del Consejo de Europa también hace hincapié sobre ello; "las preguntas formuladas por el asegurador deben ser claras y comprensibles, directas, objetivas y precisas" (principio 1, punto 9).

extralimite de lo establecido en la ley 41/2002 (Art.16) y de los fines legalmente establecidos se podría considerar ilícito y que vulnera el derecho fundamental de protección de datos de las personas. Es más, "los datos, valoraciones e informaciones que ésta contiene superarán ampliamente el conocimiento necesario para cualquiera de los usos posibles de los datos relativos a la salud en el ámbito asegurador" (ALVAREZ, 2006, 27)[945]. No cabe duda que puede afectar al derecho a la autodeterminación informativa, es decir, el derecho de control que el individuo posee sobre sus informaciones de carácter personal.

6.4.2. Deber de información.

En la recogida de los datos sobre la salud mediante impresos (o en el interfaz de la aplicación) deberá figurar la información del art. 13 RGPD[946] [947]

[945] Álvarez González, S.. La utilización de datos genéticos por las compañías aseguradoras. Instituto de Ciencias del Seguro. *Fundación Mapfre*. 2006. Pag 27. Recuperado de http://fundacionmapfre.com/ccm/content/documentos/fundacion/cs-seguro/libros/la-utilizacion-de-datos-geneticos-por-las-companias-aseguradoras-106.pdf

[946] Señala el art. 13.2 RGPD; "a) la identidad y los datos de contacto de la aseguradora y, en su caso, de su representante; b) los datos de contacto del DPO, en su caso; c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento (consentimiento, ejecución del contrato, etc.); d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero; e) los destinatarios o las categorías de destinatarios de los datos personales, en nuestro caso; los *datos de salud*; f) en su caso, la intención del responsable de realizar transferencias internacionales". El apartado 2 del art. 13 establece que el responsable del tratamiento (la aseguradora de salud) facilitará al interesado (candidato a asegurado), en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos *leal y transparente*: a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo; b) la existencia del derecho a solicitar a la aseguradora el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos; c) cuando el tratamiento esté basado en el consentimiento (artículo 9, apartado 2, letra a)) se informará al interesado la existencia del *derecho a retirar el consentimiento* en cualquier momento; d) el *derecho a presentar una reclamación* ante una autoridad de control; e) si la *comunicación de datos personales* es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado *está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos* (algo muy importante para este sector); f) la *existencia de decisiones automatizas*, incluida la elaboración de perfiles e *información significativa sobre la lógica aplicada*, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado. Y el apartado 3 señala que; "cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, *proporcionará* al interesado, con anterioridad a dicho tratamiento ulterior, *información* sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2".

[947] Las aseguradoras deben tener garantías adecuadas para el almacenamiento de los datos personales relativos a la salud; "los aseguradores no deberían almacenar información personal relacionada con la salud *que ya no es necesaria* para el cumplimiento de la finalidad para la cual fueron recogidos. Deben, en particular, no almacenar datos personales relativos a la salud si se ha rechazado una solicitud de seguro, o si el contrato ha expirado y reclamaciones ya no se pueden hacer" (punto 12). Este punto hace referencia al art. 5.1.e RGPD ("limitación del plazo de conservación"). También señalan algo muy

6.4.3. Fuentes de datos.

Me parece interesar destacar lo que se señala en la Recomendación del Consejo de Europa respecto a que los datos salud obtenidos en el *dominio público,* como en las redes sociales o foros de internet (por ejemplo, *Fb* o *Patientlikeme*), no deberán permitir evaluar los riesgos o calcular las primas.

6.4.4. "Deber de declarar" vs "deber de responder", "derecho de supresión o derecho de oposición" del titular y candidato asegurado.

Comunicar esta información tan sensible por parte de determinados grupos sociales puede suponer consecuencias gravosas y negativas. Según la *Asociación francesa la liga contra el cáncer*, "el 62% de los encuestados declara que a menudo se encuentran con problemas financieros después de la enfermedad y el 82% que es más difícil encontrar un préstamo bancario o un seguro"[948], habida cuenta su situación y posible "riesgo" de reincidencia de la enfermedad.

Por un lado, me parece interesante diferenciar como ha señalado algún autor[949] que más que tratarse de un *deber de declarar*, consiste en un *deber de responder del tomador*. Esto es una cuestión diferente a la "ocultación" de determinados datos médicos como podría ser la superación de una enfermedad de cáncer hace 10 o 20 años por el asegurado, "determinantes para la conclusión del contrato"[950] (STS 799/2002, de 26 junio).

Y por otro lado, es necesario precisar dos cuestiones. En primero lugar, desde un punto de vista etimológico que no se trata *per se* del *derecho de supresión* del

interesante y que supone el preludio del objeto de la nueva normativa ("accountability") y es que las aseguradoras deberían adoptar *reglamentos internos* para proteger la seguridad y confidencialidad de los datos relacionados con la salud de la persona asegurada. En particular, los datos personales relativos a la salud deben ser almacenados con acceso limitado por separado de otros datos, y los datos guardados para fines estadísticos deben ser anónimos (punto 13). Y además se deberían realizar auditorias externas e internas (punto 14).

[948] Vid. https://translate.google.es/translate?hl=es&sl=fr&u=http://www.20minutes.fr/sante/1563619-20150316-droit-oubli-survivants-cancer-projet-loi-sante&prev=search

[949] Arroyo Martínez, I. (2003). Ley de Contrato de Seguro, p. 35. Madrid : Tecnos.

[950] Vid. SSTS 799/2002, de 26 de julio ("el dolo que se aprecia es, evidentemente , de naturaleza negativa, en cuanto supone reticencia en la obligada que silenció los hechos y circunstancias influyentes y determinantes de la *conclusión del contrato*, que de haberlos sabido la otra parte influirían decididamente en su voluntad de celebrar el contrato (...), conceptualización del dolo a la que responde la conducta del asegurado al contestar el cuestionario que le fue sometido silenciando el padecimiento que sufría y que requería un tratamiento diario" [F.J. 4])..

Reglamento sino en todo caso más bien de un *derecho de oposición,* puesto que el interesado lo que pretendería es negarse a dar traslado o comunicar que ha padecido una enfermedad antigua. Pero más que poner el punto de mira en el derecho de protección de datos sería conveniente tener una visión extensiva desde el punto de vista de la autodeterminación informativa. En segundo lugar, deberíamos precisar la diferencia entre *el derecho de protección de datos y la autodeterminación informativa.* Esta última tiene la función *de garantizar* a los ciudadanos unas *facultades de información, acceso y control de los datos* que les conciernen y en cambio, el primero se centra en el deber de *acciones positivas* que recae tanto sobre los poderes públicos como sobre los agentes privados.

En todo caso y aunque se pueda intuir no se podrá considerar responsable (o infractor) del "deber de declarar" al candidato de asegurado que no comunique esa información si estas no han solicitado rellenar el cuestionario previo o se ha realizado un cuestionario previo (Stc Tribunal Supremo 469/1997, de 31 de mayo, o 498/1993, de 18 de mayo). Algo que se puede extender a la situación de uso obligatorio de dispositivos wearables.

En todo caso, a mi juicio, en este escenario no se pretende "sacrificar" los intereses de las aseguradoras sino "ajustarlos" a la realidad menos gravosa y minimizar los riesgos de impacto en el derecho fundamental del individuo, que en caso de ponderación el derecho a la autodeterminación informativa de los pacientes no se debería ver sacrificado por el derecho a solicitar información de las aseguradoras.

A mi modo de ver para otorgar seguridad jurídica a las personas debería regularse el "derecho de explicación" como ocurre ya en EEMM con las decisiones automatizadas; y en todo caso, ampliar el alcance del deber de información de las aseguradoras lo máximo posible en situaciones donde los *dispositivos wearables* (con naturaleza similar a los "cuestionarios clásicos") toman decisiones automatizadas determinantes para los derechos y libertades de las personas (Ver capitulo 2, problemas de transparencia: elaboración de perfiles y decisiones automatizadas).

6.4.4.1. Acceso información personal de salud de ex pacientes con enfermedad graves. Caso de Francia.

Existe un debate respecto a la posición de las aseguradoras, mutuas profesionales, etc. frente *al acceso de los datos de salud de ex pacientes con enfermedades graves.* Una orden ministerial de salud de 2013 prohibió el acceso a la base de datos del Sistema Nacional de Seguros de Salud para asalariados

(*Sniiram*) a los organismos con fines de lucro como las compañías de seguro o laboratorios farmacéuticos, pero fue considerada ilegal por el Consejo de Estado quien solicitó que se anulara. Finalmente, tres años después, la orden ministerial se modificó y "se abrió el acceso a cualquier organismo de investigación (público y privado) tras aprobación del Instituto de datos y autorización de la *CNIL*" (Autoridad francesa de protección de datos)[951] [952]. En este sentido y volviendo a la jurisprudencia española, ¿se podría considerar *"ocultación de mala fe"* si no hay solicitud o reconocimiento médico? A mi entender no podría entenderse como ocultación si no hay nada que ocultar o responder. Otro asunto sería intentar "ocultar" la información *comunicada* por parte de los centros sanitarios, por ejemplo, a través del historial clínico. Entendido de esa manera parece pretender más que el derecho de cancelación el "derecho a oposición de cesión de datos a terceros" (de centros de asistencia sanitaria a la aseguradora).

Acaso, *¿no sería posible un "derecho a ser olvidado" en el ámbito de la salud?* En Francia, ya es una realidad desde el 2015 para estas personas[953] no sólo para las personas con patología de cáncer sino también para todas las enfermedades crónicas[954] "*siempre que el progreso terapéutico y los datos de la ciencia demuestra la capacidad de los tratamientos en cuestión para limitar de manera significativa y duradera sus efectos*".

6.5. Datos genéticos y aseguradoras.

Recientemente vimos el poder de la base de datos genéticos hasta el punto que una empresa de teste genéticos (FamilyTreeDNA) ha reconocido que cedía sus datos de sus clientes a la FBI para ayudar en investigaciones criminales y otra empresa genetista (23andMe) vendió su base de datos a una farmacéutica por 300 millones de dólares[955]. Por su parte, el sector asegurador también intenta aprovechar las bondades de la fuente

[951] *Supra cit*. (Debíes)

[952] Así las cosas, el decreto del 26 de diciembre del 2016 de creación del tratamiento de datos personales de *salud sistema nacional de datos de salud* estableció las autorizaciones de acceso a la base: *datos totalmente anonimizados* en libre acceso para su re-uso, con fines de democracia sanitaria, pero también de creación de nuevos servicios por parte de las empresas. La conformidad de estos datos, muy agregados, a las necesidades del público se comprobara con el tiempo; *acceso a datos agregados* para fines de investigación, estudio o *evaluación de interés público*, bajo autorización del Instituto nacional de los datos de salud y de la CNIL; acceso permanente exhaustivo por parte de *servicios públicos designados y agencias sanitarias*.

[953]Girard-Opicci, C. (10 de febrero de 2015). Los ex pacientes de cáncer o las personas con enfermedades crónicas pueden beneficiarse de un seguro de "derecho a olvidar**". *Net-Iris.*** Para más info aquí
("Las personas que hayan padecido cáncer pueden estar ***exentas de reportar*** *su antigua enfermedad* a la aseguradora bajo ciertas condiciones: para los cánceres que ocurren antes de los 15 años, 5 años después de la fecha final del protocolo terapéutico; para todas las afecciones cancerosas, 15 años después de la fecha final del protocolo terapéutico; de acuerdo con una tabla de referencia para personas que han sufrido ciertos tipos de cáncer cuando la fecha final del protocolo terapéutico es inferior a 15 años").

[954]Les cles de la banque. Proyecto de ley 2015 aquí. No obstante, anteriormente, con el acuerdo AERAS (Aseguramiento y Préstamo con Riesgo de Salud Mejorado), firmado en 2007 entre las autoridades públicas, los profesionales de banca y seguros y las asociaciones de pacientes y consumidores, se pretendía facilitar el acceso a seguros y **préstamos** para personas que tienen o han tenido un problema de salud grave**".**

[955] Vid. https://www.eldiario.es/sociedad/test_geneticos-ADN-privacidad-ciencia_0_869313773.html

de información basada en datos genéticos, de hecho, el desarrollo científico y tecnológico puede modificar las previsiones técnicas en los seguros de Salud. Ahora bien, ¿sería admisible un acuerdo entre asegurador y asegurado que extendiera el deber del tomador al sometimiento de análisis genéticos necesarios para comprobar su predisposición a enfermedades relevantes? Son inevitables tanto el conflicto de intereses entre aseguradoras y candidatos a un puesto de trabajo como la evolución y desarrollo de las pruebas genéticos en el futuro cercano.

Pero, ¿de qué manera afectaría a los candidatos? Ellos pueden no estar interesados en conocer su propia predisposición genética, *"el derecho a no saber*", ya que el resultado adverso de una prueba genética puede influir negativamente en su bienestar emocional (HERRERA, 2010,61). Desde un punto de vista ético hay otra cuestión y tiene que ver con la comunicación *in personan* de esa información (sin tener que producirse de cesión de datos) y la buena fe en el contrato de seguros. Aunque lo más polémico tiene que ver con la discriminación que puede producirse como comentaremos en el capítulo de Ética, que derivaría a que existieran grupos de ciudadanos de primera, de segunda, etc. A pesar de que no existe en España una norma que trate sobre la realización de pruebas genéticas por compañías de seguros ni a la utilización de la información genética que el asegurado, se podría acudir a los textos internacionales y europeos:

i. La Convención de Derechos Humanos y la Biomedicina (1997) establece que; "los análisis predictivos de enfermedades genéticas que permitan identificar a una persona como portadora de un gen responsable de una enfermedad, o bien detectar la predisposición o susceptibilidad genética o una enfermedad, <u>sólo</u> *podrá hacerse por motivos de salud o de investigación científica relacionada con motivos de salud*, contando con un asesoramiento genético apropiado. (Art.12).

ii. La Recomendación del Comité de Ministros (Consejo Europa, 2016) señala que "los datos predictivos actuales como resultado de las pruebas genéticas no deben ser procesados a efectos del seguro salvo que esté autorizado por la ley".

<u>Ni en la LOPDGDD ni en el RGPD (ni en leyes sectoriales) parece el legislador señalar disposición alguna expresa sobre datos genéticos haciendo referencia al sector de las aseguradoras</u>. Parece lógico que las disposiciones normativas que estén por venir no deberían permitir una suerte de "derecho a exigir" pruebas genéticas sobre las expectativas de salud del asegurado o de su familia como condición previa para la celebración del contrato de seguro. Esto constituiría un potencial mecanismo de

discriminación, y atentaría contra los derechos fundamentales y libertades de las personas y asegurados.

CAPÍTULO VIII. IMPLICACIONES ÉTICAS DESDE EL PUNTO DE VISTA DE LA PROTECCIÓN DE DATOS Y LA PRIVACIDAD EN LA INDUSTRIA DEL CUIDADO DE LA SALUD DIGITAL.

SUMARIO: 1. CONSIDERACIONES INICIALES.- 1.1.Dataísmo, fuentes de datos de salud y stakeholders. 1.2.La medicina participativa, el negocio farmacéutico y la ética (de datos). 1.3.Los derechos fundamentales, ética y privacidad.2.IMPLICACIONES ÉTICAS Y DE LA PRIVACIDAD EN SALUD.- 2.1.Implicación ética con Big Data. 2.2.Implicaciones éticas con IA. 2.3. Implicaciones éticas con IoT y m-Health. 2.4.Implicaciones éticas con Blockchain/DLT. 2.5.Implicaciones éticas del futuro: neuroinformática, neurotecnología y biohacking, informática cuántica y genética. 3.LA ETICA DE LOS DATOS Y LAS PERSONAS.- 3.1.Preocupación por la privacidad.. 3.2. El titular como propietario del dato personal. 3.3.Mercado negro de datos de salud. 3.4.Datos personales para el bien común. 4. LA ÉTICA DE LOS DATOS Y LAS ORGANIZACIONES.- 4.1.La ética de los datos y RSE. 4.2.La ética impuesta. 4.3.Comités de ética en empresas. 4.4. La necesaria autoevaluación. .4.5.Certificaciones y sellos de calidad de ética de datos. 4.6.Ética desde el diseño ("Ethic by design") 4.7.Los valores y la ética de datos. 4.8.La privacidad como valor..4.9.Casos de estudio 4.10.Conclusión: "De las reglas a los valores, de la amenaza a la identidad corporativa". 5. LA ETICA DE LOS DATOS Y LAS INSTITUCIONES PÚBLICAS Y GOBERNANZA.

"La ética puede ser la obra de arte más grande de la humanidad"

Giovanni Butarelli (2018)

1. CONSIDERACIONES INICIALES.

El SEPD, *Giovanni Butarelli*, en el 2018, señaló que *"las éticas son valores* compartidos que cambian con el tiempo y difieren entre sociedades e incluso individuos; pero trabajamos continuamente para armonizarlos a través de varios mecanismos de socialización, algunos conscientes, otros menos". La ley y la ética pueden tener similitudes en sus funciones como guías ya que nos indican lo que esté bien o mal, lo que es justo o no pero, también, diferencias según él: "la ética es un

acuerdo informal ampliamente compartido sobre cómo debemos comportarnos como seres sociales y las leyes son necesarias para definir oficialmente este acuerdo, hacerlo visible y hacerlo cumplir a través de sistemas de sanción donde no se mantienen. Las leyes surgen de una fuente de ética, se podría decir".

¿La ética[956] está relacionada con la moral o con la legalidad? ¿sólo es incorrecto aquello que está prohibido por la ley? Ya no es únicamente necesario cumplir la ley, y demostrarlo, sino que el debate se traslada a la dimensión más ética, filosófica y moral que pueda existir.

Existe una dimensión de la ética que se desarrolla en el ámbito de los datos de las personas, su utilización y de los derechos y libertades de éstas. Centrémonos en esta dimensión.

Para los autores *Floridi y Taddeo* (2016)[957], la ética de datos se trata de "una nueva rama del ética que estudia y evalúa los *problemas morales relacionados con los datos* (registro, tratamiento, difusión, etc.), *algoritmos* (incluida la inteligencia artificial, ,el aprendizaje automático y los robots) *y prácticas correspondientes* (incluidas las prácticas responsables de innovación, programación, hacking y profesionales de los códigos), con el fin de formular y apoyar *moralmente buenas soluciones* (por ejemplo, conductas correctas o valores correctos)".

Según *Tranberg y Hasselbach* (2018) [958] de la *Thing to tank Dataethics* se trata de "un *uso responsable y sostenible de los datos*, de hacer lo correcto para las personas y la sociedad". A continuación, añaden que; "la ética de los datos se refiere y se adhiere a los principios y valores en los que se basan las leyes de protección de datos personales

---

[956] Ahora bien, me pregunto,también *¿por qué podríamos necesitar de la ética?* La ética nos asiste en la toma de decisiones hacia el bien a lo largo de nuestra vida y aparece ahí donde no puede llegar la ley y su dimensión es muy relevante e imprescindible. Ya dos décadas atrás empezó a existir una cierta tendencia de "ética verde", donde había escépticos que pensaban que quizás la preocupación por la sostenibilidad ambiental no llegaría nunca a la sociedad, a las autoridades o a los altos mandos de las empresas. Ahora es más que una realidad, no sólo porque la podemos encontrar en las placas solares que calientan hogares y edificios de empresas o en los vehículos eléctricos o en las políticas de RSE y política de economía circular de las grandes organizaciones, sino también porque ya éstas pueden contar con *best practices* o negocios verdes (por ejemplo, *cloud green*) y ser a su vez, supone una ventaja competitiva. Se está produciendo un cambio de paradigma ético que se manifiesta casi, como movimiento social producido por el desarrollo tecnológico que vivimos.

[957] Floridi, L., Taddeo, M. (2016). What is data ethics? Phil. Trans. R. Soc. A 374: 20160360. Recuperado de http://dx.doi.org/10.1098/rsta.2016.0360

[958] Tranberg, P., Hasselbalch, G. (2018). DataEthics – Principles and Guidelines for Companies, Authorities & Organisation. Recuperado de https://dataethics.eu/wp-content/uploads/Dataethics-uk.pdf

y derechos humanos". Y no sólo eso, para las autoras, la ética de los datos "es un paso más allá del mero cumplimiento de las leyes de protección de datos personales: todo el tratamiento de datos respetará como mínimo los requisitos establecidos en el RGPD, la Carta de los Derechos Fundamentales de la Unión Europea y la Convención de Derechos Humanos de la Unión Europea".

Pero para entender mejor de qué trata la ética de los datos será necesario hablar de los *principios* que estipulan estas autoras:

i. "*El ser humano en el centro.* Los seres humanos siempre prevalecen sobre los intereses institucionales y comerciales (y deben ser los principales beneficiarios del tratamiento de datos).

ii. *El control de los datos individuales.* Los seres humanos deben tener el control de sus datos y estar autorizados para gestionarlos.

iii. *La transparencia.* Las actividades de tratamiento de datos y las decisiones automatizadas deben ser verdaderamente transparentes. El propósito y los intereses, riesgos, consecuencias sociales y éticas del tratamiento de datos deben ser claramente entendidos por parte de los titulares de datos.

iv. *La responsabilidad.* La rendición de cuentas es muy importante en la protección de datos. Las autoras hablan de un tratamiento de datos *sostenible* integrado en toda la empresa y que garantiza una responsabilidad ética a corto, medio o largo plazo.

v. *La igualdad.* Las autoras hablan de tener en cuenta a las personas vulnerables que pueden ver afectadas su autodeterminación o exponerlos a discriminación o estigmatización relacionadas con cuestiones de salud, por ejemplo".

Ahora bien, ¿dónde estarán los límites morales y éticos de la implantación tecnológica en nuestra sociedad? ¿cómo pueden los individuos -como *responsables de sí mismos*- controlar la situación? ¿qué parámetros éticos habrá que trasladar a los desarrolladores de tecnología y a las organizaciones empresariales?[959].

[959] La tecnoética intenta dar respuestas que se producen durante el desarrollo de la nueva tecnología y su aplicación por las personas y para las personas. Pensemos en los comités éticos internos corporativos por parte de los desarrolladores en el desarrollo de una *app* para la secuenciación del genoma o de edición genética CRISPR. La tecnoética, en este sentido, podría convertirse en un instrumento para la regulación y la guía para utilizar el poder de la tecnología en la dirección correcta. Además, con la llegada de los avances tecnológicos los principios de tecnoética se enfrentarán al cambio continuo. La tecnoética es la especialidad de la ética que se ocupa de las implicaciones morales de las aplicaciones de la tecnología (vid. https://es.wikipedia.org/wiki/Tecno%C3%A9tica). En este sentido conviene señalar algunos de esos *aspectos morales* de la tecnología: (i) *"El utiliatarismo.* Se encuentra reflejado en tecnologías que mejoran la calidad de vida y limitan los efectos colaterales negativos de esta. La realidad virtual nos permitiría en teoría vivir una vida compuesta sólo de placer pero alienando la realidad como consecuencia; (ii) *Filosofía kantiana.* Según la filosofía kantiana la tecnología debería ser un bien en sí misma y no debería ser simplemente explotada como un medio; (iii) *Filosofía hobbesiana.* La tecnología permite restaurar la libertad al darnos mayor facilidad de movimiento, permite reducir las distancias y facilita la comunicación; (iv) *Filosofía de Lévinas.* Es posible ponerle un rostro a problemas que ocurren

1.1. Dataísmo, fuentes de datos de salud y stakeholders

1.1.1. ***El dataísmo.***

Hace tiempo los pensadores humanistas defendían que la libre voluntad era lo más importante. El principio de libre albedrío (de la deformación vulgar del vocablo latino *arbitrium*) ha sido criticada como corriente o ideología puramente individualista acompañada de implicaciones éticas (donde las personas eran responsables de sus propias actuaciones, jurídicas, científicas, psicológicas o religiosas). La libertad, don excelente de la Naturaleza, propio y exclusivo de los seres racionales, confiere al hombre la dignidad de estar en manos de su albedrío y de ser dueño de sus acciones[960].

El filósofo *Spinoza*[961] señaló que "las decisiones de la mente no son nada salvo deseos, que varían según varias disposiciones puntuales". Este autor añadía que "los hombres se creen libres porque ellos son conscientes de sus voluntades y deseos, pero son ignorantes de las causas por las cuales ellos son llevados al deseo y a la esperanza". Por su parte, *Schopenhauer* [962], siguiendo la línea de Spinoza, señala que las personas se creen libre pero a posteriori "se dan cuenta —a su asombro— de que no son libres, sino sujetos a la necesidad"[963].

Los modelos comerciales, también en el sector del mercado de la salud digital, están explotando nuevas formas de recolección masiva, transmisión instantánea, combinación y reutilización de información personal para fines imprevistos y con dudosas y opacas políticas de privacidad.

---

al otro lado del mundo y aportar ayuda rápidamente. Por supuesto, el otro lado del poder de las telecomunicaciones es la distorsión de la información y uso de la propaganda para alienar a otros; (v) *Filosofía de Foucault.* Para poder tener objetivos claros para actuar, primero se debe tener un completo conocimiento de sí mismo. Con el entendimiento propio podemos ponernos en el lugar de otros y así poder abordar problemas de distintos ángulos y prever problemas sociales."

[960] Pero lo más importante en esta dignidad es el modo de su ejercicio, porque del uso de la libertad nacen los mayores bienes y los mayores males. Sin duda alguna, el hombre puede obedecer a la razón, practicar el bien moral, tender por el camino recto a su último fin. Pero el hombre puede también seguir una dirección totalmente contraria y, yendo tras el espejismo de unas ilusorias apariencias, perturbar el orden debido y correr a su perdición voluntaria (Carta Encíclica *Libertas Praestantissimum* León XIII, 1888). Vid. http://w2.vatican.va/content/leo-xiii/es/encyclicals/documents/hf_l-xiii_enc_20061888_libertas.html

[961] Spinoza, Baruch, *Ethics* , Libro III, página 2, nota; Libro II, página 48; Libro I, apéndice en Wikipedia.

[962] Schopenhauer, Arthur, *The Wisdom of Life* , p 147 en Wikipedia.

[963] Schopenhauer. Freedom Of the Will, Cap. II.

El (aparente) deseo de acceder a la máxima información posible y participar en el flujo continuo de datos (entre individuos, empresas, gobiernos, stakeholders, etc.) hace que los individuos actúen de "forma complaciente", e incluso en ocasiones, contrarios a su voluntad.

"Los gobiernos y las empresas pueden ir más allá de los 'datos minería 'a' minería de realidad', que penetra en la experiencia cotidiana, la comunicación e incluso el pensamiento" (Nathan, 2006)[964].

El deseo deja de ser voluntad y se convierte en mera necesidad encubierta. Si pensamos que nuestra mayor necesidad vital es "mantenernos con vida o buscar los mejores medios para nuestra salud, posiblemente a las personas no nos importe renunciar a nuestra privacidad. Esto es lo que predice *Harari*[965]. Entonces, ¿es necesaria una ponderación entre el derecho a la vida o la protección de la salud y el derecho fundamental de la protección de datos personales?

Parece que por su parte, el profesor y filósofo *Harari*, cree que esa libre voluntad para dirigir el rumbo de nuestras decisiones (en forma de deseos) para satisfacer nuestras necesidades, podría acabar "truncada" con la llegada de la tecnología (y sus lobbys). Él señaló que "los gurús de la alta tecnología y los profetas de *Silicon Valley* están creando una nueva narrativa universal que *legitima la autoridad de los algoritmos y el Big Data*". Con toda la información –personal- almacenada en la Red, serían capaces de ofrecer un único producto o servicio diseñado a medida para los clientes sin ni siquiera preguntarles. Es decir, "el *dataísmo* producirá una *customización al milímetro de lo que nos ofrecerá el mercado"*.

---

[964] Nathan Eagle, Alex (Sandy) Pentland (marzo de 2006). Realización de minería: detección de sistemas sociales complejos. Journal Personal and Ubiquitous Computing. Vol. 10, edic. 4, págs. 255-268. Shoshana Zuboff en *Big Other: vigilancia del capitalismo y las perspectivas de una civilización de la información*, Journal of Information Technology (2015) 30, pp. 75-89.
Esta autora escribe: "Como resultado de la mediación informática generalizada, casi todos los aspectos del mundo es representado en una nueva dimensión simbólica a medida que los eventos, los objetos, los procesos y las personas se vuelven visibles, cognoscibles y compartibles de una manera nueva ". Zuboff concibe el "surgimiento de una nueva arquitectura universal" que ella llama "Gran Otro", un régimen ubicuo de instituciones en red que registra, modifica y mercantiliza la experiencia cotidiana, desde tostadoras hasta cuerpos, comunicación y pensamiento, todo con miras a establecer nuevas vías para la monetización y el beneficio" (pág. 77)

[965] Ver más info en : https://es.wikipedia.org/wiki/Homo_Deus:_Breve_historia_del_ma%C3%B1ana

¿Estamos entonces inevitablemente ante la desaparición del individualismo? Algunos autores creen que "podría enfrentarse el cerebro humano como procesador biológico desfasado contra los (súper) procesadores electrónicos" [966].

Por su parte, el filósofo *Byuyng-Chul Han*[967] dice que "estamos en pleno *dataísmo:* el hombre ya no es soberano de sí mismo sino que *es resultado de una operación algorítmica* que lo domina sin que lo perciba; lo vemos en China con la concesión de visados según los datos que maneja el Estado o en la técnica del reconocimiento facial". Harari sigue la misma línea al declarar que "los organismos no son sino algoritmos, por tanto, pudiera suceder que en un universo en el que el paradigma dominante sea el *dataísmo* donde el homo sapiens pierda su preeminencia". Harari[968] plantea que "podemos interpretar que toda la *especie humana es un sólo sistema de procesamiento de datos*, siendo cada uno de los seres humanos un chip" y "una vez que los sistemas Big Data me conozcan mejor de lo que yo me conozco a mí mismo, la autoridad se desplazará de los humanos a los algoritmos"[969].

Comparando el dataísmo como si se tratara de una religión, *Harari* predice que el *credo dataísta* convertirá a las personas en *fieles de la información*.

En este sentido, *Steve Lohr*, autor de la obra *Data-ism,* se pregunta: *¿qué están haciendo los grandes datos por nosotros? ¿qué podrían hacer? ¿qué deberíamos dejar de confiarle?* [970]. Este es un gran dilema que abre un amplísimo debate.

El principio fundamental del dataísmo es la defensa del flujo de datos y la defensa a ultranza de la libertad de la información. Desde mi opinión, como se puede sospechar, surgen ciertas críticas en torno al *dataísmo*:

- *Respecto al problema de la consciencia humana individual y colectiva*. Existe el riesgo de que el individualismo desaparezca. La creatividad, la innovación y las

[966] Peña Corrales, P. (19 de octubre de 2016). Dataísmo: ¿El albor de una religión digital?. *La Grieta.* Recuperado de http://lagrietaonline.com/dataismo-el-albor-de-una-religion-digital/
[967] Geli, C. (7 de febrero de 2018). "Ahora uno se explota a sí mismo y cree que está realizándose*". El País.* Recuperado de https://elpais.com/cultura/2018/02/07/actualidad/1517989873_086219.html
[968] HARARI, Yuval Noah (2017). *Homo Deus: A Brief History of Tomorrow*. UK: Vintage, Penguin Random House. p. 440.
[969] HARARI, Yuval Noah (2016). Yuval Noah Harari on big data, Google and the end of free will. *Financial Times*. Recuperado de https://www.ft.com/content/50bb4830-6a4c-11e6-ae5b-a7cc5dd5a28c
[970]Vid. https://www.washingtonpost.com/opinions/you-can-run-from-big-data-but-can-you-hide/2015/03/20/082ea46c-c805-11e4-a199-6cb5e63819d2_story.html?noredirect=on&utm_term=.cc5c1476d724

libertades pueden estar en riesgo. Los individuos tienen derecho a ser autónomos, es decir, a tener capacidad de obrar, facultad de enjuiciar sus actuaciones y de responder por sus consecuencias. "El futuro privilegiado de las nuevas tecnologías quedará en manos del gobierno y de grandes empresas y a costa de ciudadanos amenazando la identidad individual y colectiva" (Richards y King, 2013, 41)[971].

- *Respecto a la amenaza distópica de la humanidad*. La autoridad será desplazada de los humanos por los algoritmos. A quien prefiere denominar esta situación como *"dictadura de los datos"* (Cukier y Mayer-Schönberger, 2013 b)[972].

1.1.2. ***La fuente de datos y stakeholders.***

Pero, ¿dónde se generan esos datos? Existen diferente fuentes de información: registros electrónicos de salud, HCE, registros a nivel individual como dispositivos, sensores, registros de redes sociales, etc. *Casandra Grundstrom*[973] reflexionó en el *MyData2018*, sobre el ecosistema de datos de salud (ver imagen inferior). Podemos imaginar las interacciones clásicas entre pacientes y proveedores de salud, pero tal y como seña la investigadora, "estamos viendo nuevas formas en las que se están generando datos sobre la atención de la salud y que están aumentando el alcance de las partes interesadas". La realidad como ya hemos ido viendo en este trabajo es que hay varias partes interesadas en acceder a los datos. *Grundstrom* señaló que "existe una desconexión entre los grupos de interés y parte de la razón se debe a los *silos de datos*".

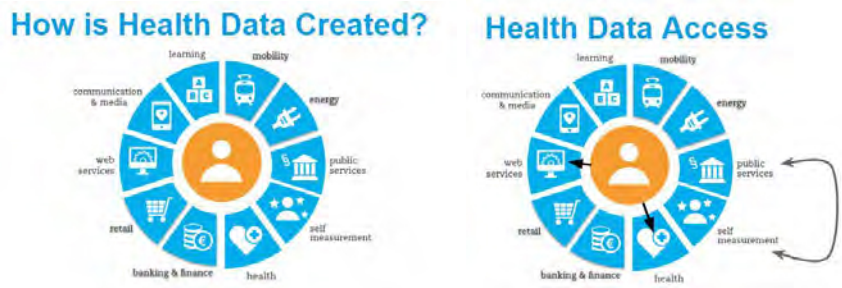


Imagen 72. ¿Cómo se crean los datos de salud? Fuente: MyData2018. Casandra Grundstrom.

---

[971] Richards Neil M. y King Jonathan H. (2013): "Three Paradoxes of Big Data", en Stanford Law Review Online.

[972] Mayer-Schönberger, Viktor y Cukier, Kenneth (mayo 2013). The Dictatorship of Data. *MIT Technology Review* . Recuperado de https://www.technologyreview.com/s/514591/the-dictatorship-of-data/ acceso en español en https://www.technologyreview.es/s/3564/la-dictadura-de-los-datos (trad. Francisco Reyes).

[973] Vid. https://docs.google.com/presentation/d/1yq9JLBufrzBIyLW2OvZRDt50TCU5tNoNoHGtyNfqVgs/edit#slide=id.g3fddd1e893_0_143

1.1.3. ***Los stakeholders.***

Corresponde a la dirección de las organizaciones realizar un análisis individualizado de cada uno de los *stakeholders* y así conocer las expectativas que pueden tener con respecto a la estrategia de la organización (Colmenarejo, 2017)[974]. Parece cierto que este papel es más importante si cabe en las Administraciones Públicas puesto que ante todo prima el interés público y el de los ciudadanos. Según la autora, "para el descubrimiento y análisis de los grupos de interés se ha adoptado la aplicación que asigna los siguientes tributos":

i. "El *stakeholder* se define como una persona, o grupo, capaz de afectar o ser afectado por la organización, es decir, es un sujeto que es interpretado por la actividad de dicha organización y que es, a su vez, "influyente", bien porque tiene poder efectivo, bien porque tiene habilidades o recursos que puede hacer valer ante la organización y afectar así a su funcionamiento. Un poder en el que es posible distinguir, a su vez, las tipologías de "poder coercitivo, poder utilitario y poder normativo-social" (Wood;Jones, 1995, 260)

ii. La urgencia con la que los *stakeholders* pueden elevar o, de hecho, elevan ante el gestor sus intereses. La urgencia puede determinarse por la capacidad de presión, determinada por su intensidad y el tiempo durante el que se hace efectiva (Mitchell et al.,1997, 867).

iii. Finalmente, los *stakeholders* quedan definidos no únicamente por su poder y su urgencia, sino también por "el grado de legitimidad de sus demandas y por el grado y tipo de responsabilidad que la empresa tiene frente a tales intereses" (Mitchell et al, 1997, 858). La legitimidad puede ser moral o legal"[975].

Pueden considerarse *stakeholders*, a mi modo de ver, por ejemplo, la industria farmacéutica, las universidades, las aseguradoras, los centros públicos de investigación médica, las asociaciones de pacientes, los gobiernos, las instituciones públicas, los hospitales, la ciudadanía, los usuarios de *wearables*, las empresas tecnológicas, los

[974] Colmenarejo Fernández, R. (2017). Una ética para Big Data. Introducción a la gestión ética de datos masivos. *Editorial UOC*.

[975] Una vez valorados estos atributos, la autora señala la posibilidad de clasificarlos de acuerdo el número de atributos y categorías (Agle et. al, 2000): (i) Los *stakeholders latentes* son aquellos que solo han sido valorados en una de las tres categorías. En el momento en el que se han realizado el análisis no tienen relevancia para la actividad de la empresa, pero eso no quiere decir que no la puedan tener en un futuro mediante la adquisición de otros atributos. (ii) Los *stakeholders expectantes* son aquellos que han sido valorados en dos de los tres tributos, su relevancia para la empresa es considerada como moderada, si bien es habitual que se presenten ante la empresa como definitivos, por su afinidad con los intereses de esta, o bien generen alianzas con otros que estén en su misma situación para llegar a adquirir el atributo que les falta para alcanzar el siguiente nivel de influencia. (iii) Finalmente, los *stakeholders definitivos* son aquellos que logran ser valorados en las tres categorías, alcanzando por tanto el nivel de influencia en la empresa.

desarrolladores, las ONGs, etc. En el futuro, blockchain y sistemas DLT posibilitará la interacción entre todos ellos con grandes ventajas como hemos visto en este trabajo.

La investigadora *Grundstrom* expuso la siguiente clasificación de *stakeholders* de la Industria del Cuidado de la Salud:

Clasificación *Stakeholders Healthcare*	**Descripción**
Los pacientes	Pacientes, o asistentes inmediatos como cuidados informales
El público	*Residentes/ciudadanos, medios de comunicación y público representativo*
Profesionales del cuidado de la salud	Centros clínicos, investigadores o médicos
Administradores	*Administradores, reguladores, gestores y organizaciones privadas*
Proveedores	Asistentes, proveedores apps, consultores, soporte técnico, y sistemas integradores

Tabla 52. Clasificación de stakeholders de la Industria de Healthcare. Fuente: *Casandra Grundstrom* (Traducción). MyData2018[976].

1.2. La medicina participativa, el negocio farmacéutico y la ética (de datos).

1.2.1. ***El e-paciente.***

Como señala el *ePatient Dave*[977], "un efecto triste del paternalismo innecesario es que impone una carga falsa a las personas responsables. En otras industrias, el valor

[976] Vid. https://docs.google.com/presentation/d/1yq9JLBufrzBIyLW2OvZRDt50TCU5tNoNoHGtyNfqVgs/edit#slide=id.g3fffc0c23d_0_0

[977] *TED. Dave deBronkart. Meet a e-Patient Dave.* Recuperado de https://www.ted.com/talks/dave_debronkart_meet_e_patient_dave (ver también https://en.wikipedia.org/wiki/Dave_deBronkart) . Conocido como *e-Patient Dave,* es un paciente de cáncer y bloguero activista por la transformación en la atención médica a través de la *medicina participativa* y *los derechos de datos de salud personal*. El impulsó y defendió la opción de transferir sus datos personales de salud en *Google Health*[977] *(Vid.* http://e-patients.net/archives/2009/04/imagine-if-someone-had-been-managing-your-data-and-then-you-looked.html) los cuales contenían mucha información errónea, medicación falsa, diagnósticos exagerados y condiciones que nunca había tenido, además el sistema no incluyó parte de información (laboratorio, alergias, etc). El problema estaba en que el hospital transmitió los datos de facturación en vez de los datos clínicos. La transferencia de información desde papel y ordenadores para posibilitar el proyecto de informatización de los registros médicos tardaría años y cientos de miñones de dólares, en cambio, los datos de reclamaciones de seguros (de facturación) por el contrario, ya están informatizados siendo más fáciles y económicos de descargar. Él declara que la comunidad de internacional de pacientes (Acorg.org) le "salvó su vida" (Vid. https://www.bmj.com/content/346/bmj.f1990) al proporcionar datos y consejos prácticos que hasta la fecha no existían en ningún artículo de una revista o sitio web del hospital. Sobre todo se interesó acerca de los efectos secundarios del tratamiento de cáncer IL-2 por melanoma metastásico. De esa comunidad, recibió 17 historias de primera mano e hizo que se sintiera preparado (psicológicamente) y su *Dr. McDermott* reconoció que el hecho de estar tan preparado ayudó a salir adelante. A su vez, el *Dr.*

está definido por el actor final (como podría ser el paciente), el que se beneficia o no del servicio, y lo mismo debería hacerse en la medicina". Desde mi opinión, el camino de transacción de la medicina paternalista del S.XIX a la medicina participativa del futuro aún está por hacer por muchos motivos (económicos, sociales, culturales).

El contexto y la autonomía del paciente en contexto internacional es positivo. Hoy en día, está en desarrollo y prueba plataformas[978] donde se ofrece al propio paciente, información personal de salud mientras está ingresado sobre la historia clínica del paciente, la medicación que se le ha prescrito, planes de cuidados, resultados de pruebas, envío de mensajes seguros, elección de menú así como acceso a información para temas de educación en salud[979].

Imagen 73. Pantallazo de ejemplo de plataforma de gestión de datos del paciente en el hospital. Fuente: Saludconcosasblog (MyChartBedside)

Veremos cómo se desarrolla, y, sobre todo, el impacto que puede tener esa medicina participativa en el *derecho fundamental de protección de datos y privacidad*.

1.2.2. ***El negocio de la Industria Farmacéutica y el valor de los datos.***

Un ejemplo de medicina participativa es *Patientslikeme*[980], una red de pacientes con fines de lucro y una plataforma de investigación en tiempo real, donde los pacientes (con más de 600.000 miembros y 100 estudios científicos de expertos y más de 2,700 condiciones de salud) es conectar con otros que tienen la misma enfermedad o afección,

---

Fergurson declaró respecto su caso que "los pacientes que ayudan en línea con una enfermedad crónica pueden ser recursos valiosos para otros pacientes con la misma afección. Por lo general, solo sabrán sobre su única enfermedad, pero como pueden dedicarle mucho tiempo, su conocimiento dentro de ese único nicho estrecho puede ser impresionante".

[978] Vid. https://journals.lww.com/lww-medicalcare/Citation/2019/02000/Inpatients_Sign_On__An_Opportunity_to_Engage.2.aspx

[979] Vid. https://saludconcosas.blogspot.com/2019/01/informacion-en-tiempo-real-para.html; ver también https://wexnermedical.osu.edu/blog/mychart-bedside

[980] *PatientsLikeMe* ha sido mencionado en más de 3.000 artículos científicos publicados e invita a participar a los investigadores en dicha empresa y siempre que es posible las investigaciones son de acceso abierto.

generando datos sobre la naturaleza real de la enfermedad. Los miembros del sitio utilizan herramientas sociales como foros, mensajes privados. El 2% de los pacientes de esclerosis múltiples están registrados en esta comunidad[981].

PatientsLikeMe permite a los miembros ingresar datos del mundo real sobre sus condiciones, historial de tratamiento, efectos secundarios, hospitalizaciones, síntomas, puntajes funcionales específicos de la enfermedad, peso, estado de ánimo, calidad de vida y más de manera continua. De hecho, han desarrollado una herramienta *("Open Research Exchange")* que permite la creación rápida de pruebas y *cuestionarios* que pueden establecer los síntomas y la enfermedad de los pacientes. En definitiva, lo que proporciona esta empresa son datos cuantitativos estructurados que se pueden agregar y utilizar para fines de investigación (por ejemplo; manejo de hipertensión, evaluación del comportamiento, idea del suicidio, etc.).

En su página web aparecen sus colaboradores; organizaciones farmacéuticas estadounidenses como *Acorda*[982] (empresa de biotecnología que desarrolla terapias para esclerosis múltiple y lesión de médula espinar) *Avanir*[983] *(trastornos del sistema nervioso central), BBK worlwide*[984] *(diabetes), Biogen Idec.*(genera más de 4mil millones de dólares al año)[985]. Pero también están otras como *partners*[986] *como Actelion, Aetna* (compañía aseguradra estadounidense que hizo convenio con Apple Watch para extraer registros de los dispositivos)*, Alexion, AstraZeneca, Boehringer Ingelheim, Bristol-Myers Squibb, Bupa, elgene, Corporación de Ciencias de la Computación, CoPatient* (intermediaria de ahorro), *Curelator headache, Denali Therapeutics, EMD Serono, FamilyWize* (intermediaria de ahorro)*, Genentech, HBG, Helsinn, inVentiv health, Janssen, Merck, Novartis, NurseTogether.com* (enfermería privada), *Pathway Genomics, Patient Power, Pfizer, RallyPoint, Sanofi, Takeda, Teva, UCB, Walgreens* (cadena de farmacias).

¿Tenemos que conformarnos con encajar una respuesta dentro del "paraguas del bien común de la investigación" ignorando el lucro cuantioso que podrían llegar a recibir en el marco de sus colaboraciones? ¿cómo sabemos que no hay intereses ocultos

---

[981] AHRQ Health Care Innovations Exchange (2008). "Las comunidades en línea fomentan el intercambio de datos, la comunicación y el aprendizaje entre pacientes con enfermedades neurológicas y otras enfermedades crónicas" . *AHRQ Health Care Innovations Exchange*. Recuperado de https://innovations.ahrq.gov/profiles/online-communities-foster-data-sharing-communication-and-learning-among-patients-neurologic

[982] Cfr. https://www.eleconomista.es/sanidad/noticias/8144868/02/17/La-farmaceutica-Acorda-se-dispara-en-bolsa-por-su-nuevo-medicamento-contra-el-Parkinson.html

[983] Cfr. https://www.patientslikeme.com/clinical_trials/NCT01767129-levodopa-dyskinesia-parkinsons-disease-AVP-923-dextromethorphan-quinidine

[984] Cfr.. http://www.appliedclinicaltrialsonline.com/bbk-worldwide-and-patientslikeme-launch-online-diabetes-health-movement

[985] Las cuales han proporcionado fondos económicos de investigación a *PatientsLikeMe*. Cfr. https://blogs.plos.org/speakingofmedicine/2012/06/14/open-access-is-not-for-scientists-its-for-patients/

[986] Vid. https://www.patientslikeme.com/about/partners

ni favoritismos entre empresas de la industria y la promoción de fármacos? ¿Cuánto están dispuestos a pagar las empresas farmacéuticas? ¿Por qué no podrían tener beneficio económico o compensación de algún tipo los titulares de datos personales de salud? [987]¿de qué manera afecta o impacta con la ética de la protección de datos y privacidad? A continuación, se muestra un pantallazo de la página abierta donde se muestran datos personales identificativos como una fotografía, género, edad, altura;

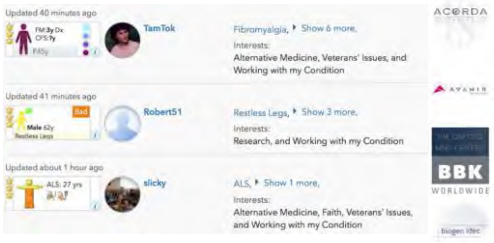


Imagen 74. Pantallazo de Patientlsikeme. Fuente: Patientslikeme

Es innegable, como decíamos el beneficio de estas plataformas pero hay que tener en cuenta el impacto que puede acarrear al derecho fundamental de protección de datos de las personas y sus libertades.

En este capítulo, no corresponde analizar el cumplimiento del RGPD de esta plataforma pero, sí, sería importante hacer una reflexión acerca del destino o finalidad de los datos personales de salud y sus tipos de tratamientos y el ciclo de vida de los mismos, asegurándonos de que no es fruto lucrativo de empresas farmacéuticas sin tener consentimiento expreso de la persona o legitimación legal. En la página web, podemos leer que: "Los datos de uso de la plataforma *por lo general* solo son utilizados por Patients Like Me y nuestros proveedores". Sin embargo cuando se deja de identificar se puede compartir con

[987] ¿Cómo se hace negocio? Según el cofundador de *Patientslikeme,* James Heywood, "el producto puede ser una publicación, el desarrollo de una nueva medida o instrumento o un informe interno para el cliente. También se genera mucho valor al colaborar en el proyecto para producir un aprendizaje compartido". Una investigación de mercado podría rondar los 100.000 dólares y un estudio de resultados HEOR podría valer de 200.000 a 500.000 dólares. Respecto a la parte ética, él justifica que sus investigaciones *ayudan a monitorear la fase IV para de medicamentos que son eficaces y están siendo utilizados por pacientes reales.* Una colaboración de 2016 con Novartis publicada en Nature Biotechnology and Value in Health exploró formas en las que los pacientes podrían proporcionar información sistemática para guiar el desarrollo de fármacos para ayudar a centrarlo más en el paciente.
(Ver *Mechas P, Lowe M, Gabriel S, Sikirica S, Sasane R, Arcona S (febrero de 2015). "Aumento de la participación del paciente en el desarrollo de fármacos". Biotecnología de la naturaleza . 33 (2): 134-5.* doi *:* 10.1038 / nbt.3145 . PMID 25658275*; ver también, Lowe MM, Blaser DA, Cono L, Arcona S, Ko J, Sasane R, Mechas P (2016). "Aumento de la participación del paciente en el desarrollo de fármacos". Valor en salud . 19 (6): 869–878.* doi *:* 10.1016 / j.jval.2016.04.009 . PMID 27712716 *.)*
Otro estudio publicado con *AstraZeneca* en 2016 ayuda a mejorar la comprensión de la enfermedad del cancer de ovario a identificar *nuevos enfoques de gestión y a generar ideas para mejorar los productos y servicios desarrollados por las compañías farmacéuticas*.
(Ver Simacek K, Raja P, Chiauzzi E, Eek D, Halling K (2017). "¿Qué esperan los pacientes de cáncer de ovario del tratamiento? Perspectivas de una comunidad de pacientes en línea". Enfermería Oncológica . 40 (5): E17 – E27. Doi *:* 10.1097 / NCC.0000000000000415 . PMID 27454765 *).*
En definitiva, según el co-fundador, lo que hacen "principalmente es *HEOR (Health Economics and Outcomes Research)* que analiza lo que les sucede a las personas con diferentes tratamientos o con diferentes afecciones y su impacto en sus vidas, resultados y productividad.". Vid. https://www.quora.com/How-much-are-pharma-companies-willing-to-pay-for-patientslikeme-data.

nuestros socios de investigación (…)". De por sí, es alarmante, el hecho de que los datos personales sean todos los siguientes; información biográfica y demográfica (fotografías no identificables, género edad, provincia), información de condición de enfermedad (fecha de diagnóstico, primer síntoma, antecedentes familiares), información de tratamiento, de síntomas, medidas (ALSFRS-R, MSRS, PDRS, FVC, Mood Map, peso, DayleMe y MonthlyMe), información de sensores, resultados de laboratorio, estado de genes individuales o variantes, respuestas de encuesta estructurada individuales y agregadas, información no identificable compartida a través de campos de texto libre (por ejemplo, evaluaciones del tratamiento, encuestas, anotaciones), conexiones con otras personas en la plataforma (por ejemplo, invitados del equipo de atención, mentores, fuentes de información, suscripciones). Además denominan a datos restringidos; el nombre, la dirección, la contraseña, el email, fecha de nacimiento, ADN (análisis de secuenciación de exoma completo o de genoma completo), dirección IP, cualquier de las anteriores que se ingresara como texto libre y los mensajes privados.

Imagen 75. Pantallazo con política de privacidad de Patientslikeme. Fuente: Patientslikeme

En junio de 2019, United Health Group Acquires

1.3.Los derechos fundamentales, ética y privacidad.

Hasta aquí todo lo relacionado con el contexto en el que nos encontramos, ahora profundicemos sobre los derechos fundamentales, ética y privacidad.

La ética deberá articularse juntamente con el Derecho a través de propuestas y soluciones, las cuales limitarán los usos poco éticos y contrarios a los derechos fundamentales de las personas, en concreto, irán dirigidas a perseguir la no

discriminación y la privacidad, y a empoderar y dar garantías al individuo. El SEPD[988], por su parte, ya establecía al inicio del texto que los derechos fundamentales a la privacidad y a la protección de los datos personales son más importantes que nunca para la protección de la dignidad humana. En la actual Era digital, el cumplimiento de la ley no es suficiente; tenemos que considerar la *dimensión ética del procesamiento de datos*[989]. De hecho, la ONU[990] en un informe del 2015, ya ha reconocido el "derecho a la encriptación" como un "derecho humano" que no debe ser socavado .

Algunos problemas éticos respecto a la privacidad (Colmenarejo, 2017) pueden ser:

i. "*Desigualdad informativa* puesto que las personas están una posición de gran desventaja ya que no tienen el mismo poder de decisión y negociación (para los contratos sobre usos de datos) que los proveedores tecnológicos, pero es que además no tienen medios para acceder y comprobar si éstos cumplen la ley.

ii. *La injusticia informativa y discriminación:* la información personal proporcionada en un determinado contexto, por ejemplo, en atención médica, puede cambiar su significado cuando se utiliza en transacciones comerciales y puede conducir a discriminación y desventajas para el usuario.

iii. *La intrusión en la autonomía moral*: la falta de privacidad puede exponer a los individuos a fuerzas externas que influyen en sus elecciones. Por ejemplo, pensemos el caso de *Cambridge Analytics*, los algoritmos sociales, algoritmos que hacen que solo se muestren entradas o noticias".

1.4.1. La moralidad, dignidad humana y privacidad de las personas.

"La ley no reemplaza a la conciencia"

Edward Snoweden

---

[988] SEPD (11 de septiembre de 2015) . Opinion 4/2015. Towards a new digital ethics. Data, dignity and technology. Recuperado de https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf También recuerda que estos derechos están consagrados en los Tratados de la UE y en la Carta de los Derechos Fundamentales de la UE, y los cuales permiten a las personas a desarrollar sus propias personalidades, llevar vidas independientes, innovar y ejercer otros derechos y libertades.

[989] *Ibidem.*

[990] ONU (2015). Informe del relator especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión. Recuperado de https://s3.amazonaws.com/s3.documentcloud.org/documents/2089684/un-encryption-report-special-rapporteur-on.pdf . (En este informe se señala que "Los Estados deben evitar todas las medidas que debilitan las garantías de las personas en el ciberespacio, como por ejemplo puertas traseras o estándares de cifrado vulnerables". El derecho de protección de datos está por encima que la vigilancia generalizada innecesaria y desproporcionada).

¿Qué posición tenemos como sujetos morales en la ética de las nuevas tecnologías? ¿deberíamos asumir la posición de sujetos morales como consumidores, como pacientes, como ciudadanos, como profesionales o empresarios? ¿o todos a la vez? Las seres humanos somos seres sociales por naturaleza y actuamos conforme a esta condición[991].

García[992] señala que "la dignidad surge en el preciso momento en que ésta empieza a existir y se convierte en parte de los valores morales del ser humano". La dignidad que posee cada individuo es un valor intrínseco, puesto que no depende de factores externos. Todo ser humano posee dignidad sin importar la condición que tenga. Y como establece *Vida-Bota*[993] "aún en el caso de que toda la sociedad decidiera por consenso dejar de respetar la dignidad humana, ésta seguiría siendo una realidad presente en cada ciudadano". Pero es verdad que el uso frecuente del concepto hace peligrar que se convierta en una expresión vacía.

Desde mi humilde punto de vista son necesarias las siguientes percepciones teniendo en cuenta el derecho de la protección de datos y la privacidad:

i. La dignidad humana *conlleva a proteger la privacidad.* La privacidad es una parte integral de la dignidad humana, y el derecho a la protección de datos fue originalmente concebido como una forma de compensar el potencial de la erosión de la privacidad y la dignidad a través del procesamiento de datos personales a gran escala (SEPD). La autodeterminación informativa alemana ya se basaba en los derechos a la dignidad y al libre desarrollo de la personalidad contemplada en su constitución.

ii. La dignidad humana *conlleva evitar las discriminaciones*. Por ejemplo, un problema importante es el de los sesgos discriminatorios en los algoritmos[994] en materia de salud, seguros y libertades

[991] Cfr. Opinion 4/2015 SEPD. "La Carta de los Derechos Fundamentales, la Declaración Universal de los Derechos Humanos y el Convenio Europeo de Derechos Humanos marcaron un antes y un después, tomado como punto de partida la inviolabilidad de la *dignidad humana.* Ésta no solo es un derecho fundamental en sí mismo, sino que también es una base para libertades y derechos posteriores, como los derechos de privacidad y protección de datos personales".

[992] García González, A. La Dignidad Humana: Núcleo Duro de los Derechos Humanos**.** *Universidad Latina de América.* Recuperado de http://www.unla.mx/iusunla28/reflexion/La%20Dignidad%20Humana.htm

[993] Vida-Bota, J. Valores y principios de la dignidad humana y sus implicaciones éticas. Ver en *Asociación Catalana de Estudios Bioéticos.* Recuperado de http://bioetica.cat/valores-y-principios-la-dignidad-humana-y-sus-implicaciones-eticas/?lang=es

[994] Knight W. (9 de octubre de 2017). *MIT Technology Review.* Recuperado de https://www.technologyreview.es/s/9610/google-advierte-el-verdadero-peligro-de-la-ia-no-son-los-robots-asesinos-sino-los-algoritmos?_ga=2.180570592.690192898.1543855212-419410505.1543855212

de las personas. La privacidad y la protección de datos son cada vez más importantes para la protección de la dignidad humana desde una perspectiva técnica, legal y ética (Ortiz, 2018)[995].

iii. La dignidad humana *no tiene precio.* Las personas no pueden ser objeto de negocios o transacciones comerciales. En este sentido, nos referimos también a nuestras identidades o avatares digitales, a nuestra información personal disponible en la Red. "El mundo es hoy un mercado en el que se exponen, venden y consumen intimidades" (Vásquez, 1999)[996].

iv. *La dignidad conlleva el respeto a las personas como individuos autónomos.* El principio de beneficencia supone respetar las decisiones, evitar causar daños y perjuicios asegurando su bienestar. Además, se deberá proteger más aún a las personas con autonomía disminuida como son los pacientes, enfermos, etc. El consentimiento informado del tratamiento de sus datos debe cumplir la normativa[997].

2. IMPLICACIONES ÉTICAS Y DE LA PRIVACIDAD EN SALUD

Según el *SEPD* (2015), la responsabilidad de dar solución al reto de la Era de la digitalización podría reposar en *un ecosistema interdependiente de desarrolladores, empresas y reguladores:*

i. *"Regulación orientada al futuro*. Por ejemplo, exigir una mayor transparencia del precio (efectivo o de otro tipo) para un servicio, puede informar y facilitar el análisis de casos de competencia, y detectar discriminación de precios injusta sobre la base de datos de mala calidad y perfilados injustos[998].

ii. *Controladores responsables*. La responsabilidad requiere implementar políticas internas y sistemas de control que garanticen cumplimiento y proporcionar pruebas pertinentes, en particular a la

[995] Ortiz, P. (2018). La protección de datos, un asunto profundamente humano. Recuperado de http://theconversation.com/la-proteccion-de-datos-un-asunto-profundamente-humano-108137

[996] Vásquez Rocca, A. Byung-Chul Han: La sociedad de la transparencia, autoexplotación neoliberal y psicopolítica. De lo viral-inmunológico a lo neuronal extresante. Nómadas. *Revista Crítica de Ciencias Sociales y Jurídicas*, N. 03. Universidad Complutense. Recuperado de hhttp://dx.doi.org/10.5209/NOMA.56074

[997] Desde el punto de vista del sector sanitario, somos conscientes del papel de función social y el componente moral importante que contiene. El principio moral de evitar el daño y el compromiso de haber el bien de manera positiva son evidencia de ello. Pero "el modelo hipocrático ya resulta insuficiente y surge la necesidad de adoptar un *nuevo código de valores* que permita responder con flexibilidad a las nuevas expectativas de la sociedad" (HASS, 2018). Vid. https://www.redaccionmedica.com/opinion/los-codigos-eticos-en-el-sector-sanitario-publico-realidad-o-ficcion--5707. Es de destacar la cita que añade este autor de CICOUREL (1983); "el paciente corre el riesgo de ser recibido como un simple receptor-elaborador de información dotado de una clara limitación lingüística-conceptual.

[998] El artículo 21 de la Carta de los Derechos Fundamentales prohíbe 'Toda discriminación basada en cualquier motivo como sexo, raza, color, origen étnico o social, características genéticas, idioma, religión o creencia, política o cualquier otra opinión, pertenencia a una minoría nacional, propiedad, nacimiento, discapacidad, edad o sexo orientación'. Muchas de estas categorías de datos ("revelan origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, sindicales y el procesamiento de datos concernientes salud o vida sexual) reciben una protección reforzada en virtud del artículo 8 de la Directiva 95/46 / CE.

supervisión independiente autoridades. Nuestro uso tecnológico genera *datos vaporosos* (Thatcher, 2014, 1770) con todas sus limitaciones, sesgos y manipulaciones. Ya el SEPD contemplo hace varios años la necesidad de cumplir el principio de limitación de finalidad del presente RGPD y la utilización de *códigos de conducta, auditorías, certificación, auditorías y una nueva generación de las cláusulas contractuales y las reglas corporativas vinculantes* pueden ayudar a construir una confianza sólida en lo digital mercado.

iii. *Ingeniería consciente de la privacidad.* Los ingenieros de sistemas y software necesitan comprender y aplicar mejor los *principios de privacidad desde el diseño* en nuevos productos y servicios a través de fases y tecnologías de diseño. La Red de Ingeniería de Privacidad (IPEN) contribuye a un intercambio fructífero interdisciplinar de ideas y enfoques.

iv. *Personas empoderadas.* Un entorno *'prosumidor'*: las personas ahora producen y consumen contenido y servicios. Las personas deben ser capaces de desafiar los errores y los sesgos injustos que hay. Los clientes no reciben una compensación justa por sus información que se comercializa. Un método alternativo para darles a los individuos un mejor control sobre sus datos, podría ser el uso de *almacenes de datos personales o 'bóvedas de datos '.* El concepto de tal *'tienda personal'* requiere mecanismos de seguridad que aseguren que solo esas entidades autorizado por el interesado puede acceder a los datos y solo a aquellas partes para las cuales son autorizado. El principio de portabilidad ha demostrado ser una poderoso habilitador para la competencia y efectivamente ha reducido los precios al consumidor cuando el mercado de telecomunicaciones fue liberalizado".

2.1. Implicación ética con Big Data

La consultora *Gartner*[999] ya predijo en su momento que en el 2018, el 50% de los negocios se producirán violaciones de ética debido al uso indebido de *big data*. La analítica de datos permite extraer conclusiones respecto a la salud que pueden repercutir en procesos de selección laboral o la interacción con las aseguradoras de salud y cambiar la vida de las personas[1000].

*2.1.1. **Análisis de los riesgos**.*

El uso de la tecnología genera datos vaporosos con todas sus limitaciones, sesgos y manipulaciones (Cotino, 2017) [1001]. De hecho, se hablan a menudo de teorías y

[999] Vid. https://www.gartner.com/newsroom/id/3144217

[1000] Cfr. Parlamento Europeo (14 de marzo de 2017). Resolución sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI)) Recuperado de http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0076+0+DOC+PDF+V0//ES Pto. 19.

[1001] *Supra Cit.*

conceptos como "armas de destrucción matemática" (O'Neil, 2016) [1002] o la "dictadura de los datos" (Cukier y Mayer-Schönberger,2013)[1003]. Está claro que, "los sistemas tecnológicos pueden tener valores sociales "incrustados" o embebidos en su diseño y que éstos sean contrarios a la igualdad, principios constitucionales y derechos humanos" (Surden, 2017,2) [10041005].

2.1.2. ***Una aproximación a posibles herramientas éticas.***

i. Evitando hacer *riesgos indeseables* para la sociedad. Es decir, implicaría analizar y conjugar desde un primer momento en el proyecto empresarial, el interés empresarial o estatal con el bien de la sociedad que supone determinado análisis de datos.

ii. Con la debida diligencia o due diligence y/o *transparencia algorítmica* (Cotino, 2017) donde los ciudadanos puedan tener derecho de acceso. Podríamos considerar un "derecho de acceso amplificado" (Miralles, 2013) [1006], ¿Por qué no?

iii. Con la *responsabilidad algorítmica*.

iv. Con equipos multidisciplinares con *profesionales de humanidades o filósofos* (Mendoza, 2017) [1007] en los comités de ética.

[1002] O'Neil, C. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, New York: Crown.

[1003] *Supra cit.*

1004 Surden, H. (13 de marzo de 2017). Values Embedded in Legal Artificial Intelligence. *U of Colorado Law Legal Studies* Research Paper No. 17-17. Recuperado de https://ssrn.com/abstract=2932333 or http://dx.doi.org/10.2139/ssrn.2932333

1005 También por ejemplo hay otros riesgos; "los datos genéticos por su propia naturaleza, van más allá de los propios individuos, sino también a su grupo familiar, incluso de colectivos más amplios relacionados social, cultural o étnicamente". Vid. González, P.A. (2017). Responsabilidad proactiva en los tratamientos masivos de datos. DILEMATA. Año 9, Nñum. 24, pp. 115-129. Recuperado de https://www.dilemata.net/revista/index.php/dilemata/article/view/412000103/493.Y es que, como dice este autor, "debido a sus condiciones técnicas solo unos pocos pueden acceder a su tratamiento y supone una concentración de conocimiento en los grandes operadores donde los interesados parecen quedar al margen".

[1006] Martin Miralles, R. (2013). Big Data vs Small low. *Congrés IDP 2013 Butlletí +Kdades: Butlletí electrònic de tecnologia, auditoria i seguretat de la informació*, Nº. 24, 2013, pp. 7-8, acceso en http://dialnet.unirioja.es/servlet/extart?codigo=4329765. Un derecho no sólo reducido a la información que contiene el responsable sino sobre qué tratamientos ha aplicado a los datos, qué información calculado se ha obtenido a partir d ellos datos y los usos concretos o las operaciones de disociaciones. Esto podría dar solución a la opacidad algorítmica.

[1007] Mendoza Zabala, G. (2017). El papel de la filosofía en la era tecnológica. Recuperado de https://www.madrimasd.org/notiweb/analisis/papel-filosofia-en-era-tecnologica

Según este autor, "los filósofos ofrecerán conocimientos sobre la lógica, filosofía de la matemática, teoría del conocimiento, antropología, retórica, argumentación, así como capacidad para enfrentarse a

2.2. Implicación ética con Big Data en las investigaciones científicas.

Un caso bastante sonado por la ausencia de ética de datos y privacidad en investigación científica fue el ocurrido con el *caso Ébola*[1008] donde se recopilaron, se dieron uso y se transfirieron internacionalmente datos de identificación personal e información humanitaria sin haber realizado un diálogo en torno a los riesgos legales.

Por su parte, la "Declaración sobre integridad científica en investigación e innovación responsable "de la Cátedra Unesco de Bioética de la UB[1009] identifica en declaraciones previas los principios de honestidad, responsabilidad, justicia *y* rendición de cuentas. A la vez propone una metodología de identificación y organización de las diversas infracciones a la integridad científica, diseñada a partir de las etapas del proceso de investigación: enunciar los objetivos, delinear las metodologías y evaluar el impacto

Llama a la atención como Francia, previamente a la entrada en vigor de la norma europea, la regulación de la modernización del Sistema de Salud donde se señalan condiciones del acceso a los datos agregados para fines de investigación que; (i) *los tratamientos de datos no deben de tener por finalidad, ni permitir en ningún momento, la identificación de las personas*; (ii) los trabajos ejecutados a partir de los datos *no deben de conducir a la promoción de productos* dirigidos a profesionales de la salud o centros de salud, (iii) ni *permitir que se excluyan garantías de los contratos de seguro o modificar las cuotas o primas de seguros*. Además, "para tener acceso a la base, cualquier organismo de investigación o estudio que desee llevar a cabo un proyecto de interés público debe someterlo al Instituto nacional de los datos de salud. Sus miembros incluyen representantes del Estado, los usuarios de la seguridad social y los productores y usuarios públicos y privados de datos de salud. El protocolo de estudio lo validará entonces un *comité científico*, antes de la autorización de la CNIL tras el análisis de los aspectos relacionados con el respeto de la vida privada" (Debíes, 2017).

i. Análisis de los riesgos.

Pongamos un caso práctico.

---

problemas de textos complejos, favorecerán el razonamiento abstracto e integrar en un discurso con sentido multitud de datos que recibamos de manera fragmentada, de muy diversas fuentes y ramas del saber, además, fomentarán el espíritu crítico ante situaciones nuevas y educarán en la necesidad de la capacidad del diálogo".

[1008] Vid. https://cis-india.org/papers/ebola-a-big-data-disaster

[1009] Casado, M, do Céu Patrão Neves, M. Itziar de Lecuona, Carvalho, A.S., Araújo J. (2016) . Declaración sobre integridad científica en investigación e innovación responsable. Cátedra Unesco de Bioética de la Universidad de Barcelona. Recuperado de http://www.publicacions.ub.edu/refs/observatoriBioEticaDret/documents/08489.pdf

Labrique et al. (2013) [1010] han observado que las appsde mHealth traen consigo beneficios pero se requiere de la aplicación de la ética. En concreto se piensa en la necesidad de crear nuevas guías de actuación o *guidelines* que den complemento a las normas y prácticas existentes. Como conclusiones sobre los riesgos deducimos lo siguiente:

- El VIH / SIDA y el abuso de sustancias conllevan cierto estigma social y comportamientos criminalizados. La EMA (o evolución ecológica momentánea) de patrones de actividad o firmas respiratorias se consideraron como *potencialmente invasivas* para la privacidad. Como solución se piensa en posibles avisos de permiso frecuentes o recordatorios de que está activada o desactivada la monitorización, además de poner límites de tiempo.
- *Destinatarios no especificados*. Los SMS mandados por los titulares de datos y pacientes son leídos indistintamente y por personas diferentes (por ejemplo, piénsese en personal sin condición médica). Hay que tener en cuenta que los investigadores son los responsables del tratamiento.
- *Duración ilimitada* del tratamiento de datos. Los mensajes permanecen almacenados durante toda la vida útil de la tecnología. Se piensa en soluciones como el Acta de Responsabilidad y Portabilidad del Seguro Médico de los Estados Unidos (HIPAA) y el certificado de confidencialidad.
- *No hay medidas de seguridad de cifrado.*

ii. Una aproximación a herramientas y recomendaciones ético-jurídicas.

a. Los comités de ética.

[1010] Labrique, A B., et al. (2013). Issues in mHealth research involving persons living with HIV/AIDS and substance abuse. AIDS research and treatment", 1-6. US National Library of Medicine. *AIDS Res Treah.* Recuperado de https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3792525/
("En VIH, varios proyectos de investigación han explorado cómo se pueden utilizar los teléfonos móviles para mejorar la adherencia al tratamiento antirretroviral en entornos de bajos recursos. El tratamiento del VIH a menudo se ve interrumpido por las recaídas en el uso de drogas, el encarcelamiento y otros factores de estrés psicosocial. La aplicación de teléfono inteligente personalizable que facilita la comunicación entre los pacientes y el personal de apoyo *y recopila datos en tiempo real que describen los factores de riesgo comunes para la falta de adherencia, como estados de ánimo negativos y uso de drogas y alcohol.* La aplicación les pedirá a los participantes que respondan a *cuestionarios breves 1-2 veces* al día para determinar el nivel de estrés que están experimentando, el consumo de drogas o los antojos. y las barreras anticipadas para asistir a las citas clínicas o cumplir con su régimen antirretroviral prescrito.") Ver también http://eterni.me/.

La Ley 14/2007, de 3 de julio, de Investigación biomédica, ya señala su labor; "ponderar los aspectos metodológicos, éticos y legales del proyecto de investigación".

No obstante, como señala el profesor Martínez (2016, 63) [1011]; "los miembros del Comité de ética no tienen suficientes conocimientos como para analizar y verificar el impacto de privacidad". Añade, además, que "no es muy habitual, que se constaten declaraciones de compromiso de cumplimiento del *Código Tipo de Farmaindustria"*.

Para el profesor será fundamental que los comités de ética:

- "Desarrollen una estrategia previa de protección de datos de datos desde el diseño y por defecto (privacy by design).
- Apliquen las herramientas de análisis de impacto en la protección de datos.
- Definan políticas de seguridad.
- Verifiquen las condiciones de tratamiento anónimo o pseudónimo de los datos.
- Preparen una información adecuada, transparente y fácilmente comprensible facilitadora de la obtención de consentimientos.
- Documenten la existencia de condiciones de cumplimiento normativo general y sectorial del proyecto.
- Cuenten con la figura necesaria del delegado de protección de datos (DPO) para que pueda garantizar el cumplimiento del principio de responsabilidad proactiva tal y como establece el RGPD" .

El profesor acierta en afirmar que "abogar y respetar la ética resulta un reto complicado que debe ser afrontado individualmente desde la *formación del personal* y considerando las estrategias que nacen en los comités de ética"(…). "El fin último de la regulación en materia de protección de datos de salud no es otro que el de evitar la *discriminación y garantizar la libertad, prevaleciendo la dignidad del paciente y el cumplimiento normativo*".

Implicar a los comités de éticas a la cultura de protección de datos y privacidad siguiendo patrones del RGPD sería la solución más adecuada.

b. El "consentimiento dinámico".

"El proceso de dar consentimiento informado en la pantalla en un entorno donde el usuario digital no tiene acceso a la consulta, a menudo implica que éste haga clic

[1011] S*upra Cit.* pp.63.

inmediatamente sin tiempo suficiente a decidir" (CIB, 12)[1012]. Por ello , se cree que un consentimiento dinámico inicial del participante en el uso de datos acompañado de sus actualizaciones sería adecuado, sirviéndose de "portales de consentimiento" (*consort portals*). Los participantes darían forma a las posibilidades de investigación a través de sus decisiones sobre qué usos quieren para sus datos.

c. Códigos de conducta.

Las instituciones, proveedores de salud (sector público) y organizaciones (sector privado) están obligadas a desarrollar *códigos de conducta o instrumentos autovinculantes* en relación a las aplicaciones de *big data* con consecuencias en caso de que se violen los principios éticos. El CIB[1013] señala que "serán dirigidas a los profesionales de salud, científicos informáticos, investigadores clínicos, científicos de datos y otras partes interesadas".

d. Atención especial a los grupos vulnerables: menores de edad y personas con discapacidad.

El CIB[1014] señala que se podrían introducir diversos modelos de consentimiento que se adecuen al contexto de la investigación.

e. Crear un sistema de vigilancia global o internacional para el uso de Big Data en aplicaciones relacionadas con la salud.

El CIB considera que "todas las Agencias nacionales de control de datos deben trabajar conjuntamente con este sistema para el uso de Big Data en aplicaciones relacionadas con la salud. Este sistema coordinado podría servir como punto de partida de un instrumento jurídico internacional sobre Protección de Datos en la Atención de la Salud y la Investigación en Salud" [1015].

f. Implicar a las instituciones internacionales, nacionales y regionales.

[1012] *Supra Cit.* pp 12
[1013] *Supra Cit.* pp 23
[1014] *Ibídem*
[1015] *Ibídem*

El CIB señala que "las instituciones que aplican estándares técnicos para dispositivos y procesos en el contexto de Big Data deben definir estos estándares de acuerdo con los principios éticos de respeto, autonomía, privacidad, y transparencia"[1016].

2.3. Implicaciones éticas con IA.

Es claro que la única forma de pasar de un enfoque de salud paliativo a uno preventivo es incrementando el volumen de datos generado y alimentando con ellos algoritmos capaces de interpretarlos de manera automatizada (Dans, 2018)[1017].

Para *Nathalie Smuha*[1018], coordinadora del grupo de expertos de la IA de la Comisión Europea: "no hay duda de que la publicación de nuestros datos puede tener consecuencias muy positivas, por ejemplo, en el desarrollo de la IA con fines médicos, sin embargo, sigue siendo extremadamente difícil proteger estos datos adecuadamente". Es aquí donde entra la ética. Concretamente, respecto al buen uso del software (en dispositivos médicos) e IA en la industria farmacéutica, es de señalar la implicación de la FDA estadounidense, creando documentos a modo de guidelines abordando cuestiones legales-éticas que afectan[1019]

Por su parte, *Miguel Luengo*[1020]*, chief data scientist* de *UN Global Pulse*, señala que los algoritmos se alimentan de los datos que los individuos dan, gracias al *big data* que generan.

[1016] Por ejemplo, se recomienda a la ONU desarrollar y adoptar un instrumento legal sobre la protección de datos en la atención médica y la investigación en salud. A la Unesco, se recomienda que desarrolle una convención sobre la protección de la privacidad, incluido un marco para nuevos enfoques de propiedad y custodia de datos personales. Y la OMS, se alienta el establecimiento de un acuerdo mediante "tiendas" sobre la presentación de apps relacionadas con la salud donde esté presenta la autonomía de las personas".

[1017] Vid. https://www.forbes.com/sites/enriquedans/2018/09/21/insurance-wearables-and-the-future-of-healthcare/#27449a671782

[1018] Vid.https://datanews.knack.be/ict/nieuws/een-nieuw-jaar-een-nieuwe-ai/article-opinion-1412987.html?cookie_check=1546692144

[1019] Vid. https://www.healthcareittoday.com/2019/06/20/fear-and-confusion-over-the-software-and-artificial-intelligence-revolution-reaches-the-fda/ y https://www.regulations.gov/docket?D=FDA-2019-N-1185

[1020] Vid. https://retina.elpais.com/retina/2019/01/04/tendencias/1546604928_551805.amp.html M.Luengo realiza una comparación metafórica interesante con el *deep learning* **como una fábrica de máscaras de escayola**, donde millones de personas están en la cola de la fábrica y el artesano de la fábrica pone un molde de escayola húmeda en la cara del primero (chica joven), del segundo (un chico), del tercero (otra

¿por qué es necesario estudiar el impacto de la IA, y en particular de los algoritmos desde el punto de vista de la ética? ¿cómo se comportan? ¿de qué manera y dónde afectan en los derechos de las personas? [1021]

2.3.1. Riesgos éticos con IA

---

chica) y así consecutivamente. De esta manera la máscara tendrá rasgos comunes a la primera y a la tercera persona.

[1021] Ahora bien, *¿qué avances regulatorios hay al respecto hasta la fecha?* El 2018 pareció ser el año del desarrollo de documentos europeos, reuniones, informes y borradores sobre guías y directrices en materia de Inteligencia Artificial y ética, sobre todo en el marco europeo. En abril se publicó una estrategia para la IA que permitiría a Europa competir con China y EEUU. Para ello, la CE creó un grupo de expertos en torno al IA para desarrollar entre otras tareas, directrices éticas para esta tecnología en Europa dirigidas a organizaciones, investigadores, organismos públicos, individuos y cualquier persone que use IA para hacer que la tecnología sea más ética. En junio de 2018, representantes de la Comisión Europea (CE) y organizaciones filosóficas y no confesionales debatieron en Bruselas sobre desafíos éticos y sociales que plantea la IA. *Andrus Ansip*, vicepresidente de la CE y responsable del Mercado Único Digital, ya adelantaba el esfuerzo que estaban realizando en inversión y en la elaboración de *las Directrices Éticas para IA basadas en la Carta de los Derechos Fundamentales de la UE*, que atenderán a los principios de protección de datos y transparencia (Vid.https://www.eldiario.es/tecnologia/CE-avanza-directrices-inteligencia-artificial_0_783572209.html#click=https://t.co/wrGOHMuiFM).

Tres meses después, en octubre de 2018, se creó la *Declaración Internacional de Ética y Protección de datos en IA* (Vid. https://www.privacyconference2018.org/system/files/2018-10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf), en Bruselas también, donde participaron la Agencia de Protección de Datos francesa (CNIL), la agencia italiana (*Garante per la protezione dei dati personali*) y el supervisor europeo de protección de datos (SEPD). La declaración señala que un desafío será la prevención de la discriminación contra las personas como resultado de las decisiones tomadas por los sistemas de inteligencia artificial, señalando que "estas discriminaciones podrían resultar en la restricción de la disponibilidad de ciertos servicios o contenidos y, por lo tanto, interferir con los derechos de los individuos, como la libertad de expresión e información, o resultar en la exclusión de personas de ciertos aspectos de la vida personal, social y profesional". Se señaló que a la hora de diseñar, desarrollar y utilizar IA y *deep learning* es necesario tener en cuenta el impacto que puede tener en el individuo, pero también en la colectividad. También, la declaración resalta varios elementos importantes para preservar los derechos humanos como la equidad, la transparencia y la privacidad por diseño. En concreto respecto a la *"ethic by design"* (punto 4), se indica que se deben: (a) implementar medidas y procedimientos técnicos y organizativos proporcionales al tipo de sistema desarrollado para respetar la privacidad; (b) evaluar y documentar los impactos esperados en los individuos y en la sociedad al comienzo de una proyecto de IA y para los desarrollos relevantes a lo largo de todo su ciclo de vida; (c) identificar requisitos específicos para el uso ético y justo de los sistemas y para respetar los derechos humanos. En el punto 5 de la declaración se señala algo muy importante a mi parecer desde el punto de vista de la cuestión que nos centra: la promoción del empoderamiento del individuo y ejercicio de sus derechos. Cuestiones que ya se han contemplado en el RGPD como el derecho de acceso o oposición (Art 15, 21 RGPD) y el derecho a objetar a no estar sujetos a una decisión basada únicamente en el procesamiento de datos automatizado (Art. 22 RGPD) garantizando el derecho a los individuos a impugnar dicha decisión y que requerirán de campañas educativas y de sensibilización. Y todo ello, utilizando las capacidades de los sistemas de IA para fomentar el empoderamiento igual y mejorar la participación pública, a través, por ejemplo, de interfaces adaptables y herramientas accesibles.

Dos meses después, en diciembre de 2018, se publicó el *Borrador de las Directrices éticas para la confianza de IA (Draft ethics guidelines for trustworthy AI)* sirviendo como documento de consulta para los *stakeholders*. Hasta aquí el resumen cronológico de la evolución de trabajos de desarrollo de esta cuestión en el marco comunitario.

Conviene decir mencionar las tres propiedades de los algoritmos (Monasterio, 2017) [1022] ;

a) *Universalidad.* Están presentes en muchas áreas de nuestra vida: consumo, política, salud, educación, etc.

b) *Opacidad o invisibilidad*. Debido a esta opacidad las personas pueden pensar los efectos negativos se han de aceptar. Las características generales que tienen los algoritmos hacen que el daño que causan sea difícil de corregir, de identificar y/o asignar responsabilidades

c) *Impacto en la vida de las personas*. Resulta acertado por parte del autor considerar a ésta la propiedad más importante y señala las siguientes dimensiones que se derivan del impacto de los algoritmos en la vida de las personas: *discriminación social, económica, de acceso libre a la información y privación de libertad y discriminación y abuso de control*. Así, por ejemplo, las minorías (raza[1023], sexo[1024], pobreza[1025]) son discriminadas por el mero hecho de serlo frente a la mayoría.

Según *Anil Aswani*[1026], ingeniero de la *Universidad de Berkley*, "los avances en IA hacen que sea más fácil para las compañías obtener acceso a los datos de salud, lo que aumenta la tentación de que las empresas los utilicen de manera ilegal o no ética". Señaló que "los empresarios o los prestamistas hipotecarios podrían potencialmente usar esta inteligencia para discriminar, por ejemplo, por estado de embarazo o discapacidad".

Así, por ejemplo, los hallazgos de un *estudio*[1027] sugieren que las prácticas actuales para *desidentificar* datos de actividad física son insuficientes para la privacidad y que la desidentificación debe agregar los datos de actividad física de muchas personas para garantizar la privacidad de las personas. Los investigadores[1028] demuestran el potencial de los datos de actividad recopilados por los relojes inteligentes, teléfonos inteligentes y rastreadores de acondicionamiento físico disponibles en el mercado para

[1022] *Supra Cit.* (*Monasterio* señala algo interesante: "los algoritmos no son neutrales, objetivos o pre-analíticos" puesto que "se enmarcan en un contexto tecnológico, económico, ético, temporal y espacial").

[1023] Vid. https://www.bbc.com/mundo/noticias/2015/07/150702_tecnologia_google_perdon_confundir_afroamericanos_gorilas_lv

[1024] Ver https://elpais.com/elpais/2017/09/19/ciencia/1505818015_847097.html

[1025] Ver https://www.xataka.com/privacidad/durante-2018-17-5-millones-ciudadanos-chinos-no-pudieron-comprar-billete-avion-tener-credito-social

[1026] Ver https://amp.infosalus.com/asistencia/noticia-inteligencia-artificial-amenaza-creciente-privacidad-datos-salud-20190104121513.html

[1027] Ver https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2719130

[1028] Ver https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2719121

contribuir a la reidentificación probabilística de los participantes de la investigación. Los datos del rastreador de actividad se unen a una larga lista de tipos de datos informados anteriormente que pueden ser identificados nuevamente.

O Pensemos por ejemplo, en *sanidad pública* y en sistemas de IA en tratamiento de enfermedades donde el algoritmo es utilizado para identificar a una persona con hepatitis C crónica para su curación. Los sistemas analizan los datos de vigilancia de la salud para controlar las tasas de tratamiento y curación dentro de un ámbito geográfico (por ejemplo, una ciudad) para evaluar el progreso. De hecho, "algunos Estados están usando algoritmos patentados aplicados al monitoreo de medicamentos recetados en bases de datos para identificar posibles compras de médicos o prescripciones inadecuadas" (*AInow*,2018)[1029]. (Ver imagen inferior)

Imagen 76. Ejemplo de plataforma IA que utilizan los profesionales sanitarios. Fuente: ApprissHealth

También hay que preocuparse por las cuestiones éticas de IA y privacidad en el ámbito de la salud, la neurotecnología y el *neurohacking*[1030]. Según el *Word Economic Forum*[1031], los científicos están alertando que IA podría hackear la mente humana y controlar los pensamientos, decisiones y emociones. De hecho, los científicos trabajan

[1029] *Supra Cit.* Pag. 7

[1030] Pero ¿qué es el *neurohacking*? Implica la aplicación de la ciencia y la tecnología para influir en el cerebro y el cuerpo con el fin de optimizar la experiencia subjetiva. Los científicos ya pueden leer los pensamientos de las personas e incluso plantar otras nuevas ideas en el cerebro, incluso en el ámbito de la atención médica. Hay que tener en cuenta la dimensión de la inversión en neurotecnología (100 millones de dólares al año) para entender lo importante que tiene que ser estudiar el impacto de esta tecnología en el sector de la Industria de la Salud, y en particular, para las personas titulares de información personal, al igual que abogar por normas éticas nuevas.. Parece evidente que los actores que pueden poner en riesgo la privacidad de las personas no son consecuentes del aspecto ético y legal que conlleva. Los investigadores, los médicos y los profesionales conectados no son responsables de las acciones no éticas.

[1031] Vid. https://www.instagram.com/p/BqfJIQDhLmr/?utm_source=ig_share_sheet&igshid=rbin43g4igsn

con un ensayo clínico de interfaz mente-ordenador ("*brain-computer interface"*) en donde si el paciente está en desacuerdo con el equipo médico, la IA "conecta" con su mente y podría leer sus pensamientos incluso aunque el paciente no haya dado la orden. Por ello, los científicos dicen que, ahora, es crucial considerar las posibles consecuencias incluido "el derecho de las personas a tener una *vida mental privada*".

Imagen 77. Neurohacking: Brain – computer interface. Fuente: Nature. World Economic Forum

Abordemos algunos casos concretos más generales , sin limitarnos al ámbito de la salud, en donde la IA impacta en los derechos de las personas.

En primer lugar, por ejemplo, la Universidad de Stanford[1032] entrenaron una red neuronal profunda ("deep learning", ver capítulo 2, aptdo. 4.1.) para predecir la orientación sexual de sujetos, *sin obtener consentimiento,* utilizando un conjunto de imágenes recopiladas de sitios web de citas en Internet. Se demostró que esa vigilancia algorítmica vulneraba los derechos de privacidad al recopilar y analizar la información personal sobre esos usuarios.

Latonero (2018) [1033] considera que la *vigilancia algorítmica* vulnera la privacidad de las personas cuyos datos se recopilan y se analizan, corriendo el riesgo de que se revele esa información personal con las consecuencias que ello conlleva.

[1032] Wangm, Y. , Kosinski, M. (2018). Las redes neuronales profundas son más precisas que los humanos para detectar la orientación sexual a partir de imágenes faciales. *Journal of Personality and Social Psichology*. Recuperado de https://psyarxiv.com/hv28a/

[1033]Lotanero, M. Governing Artificial Intelligence: Upholding human rights & dignity. *Data & Society.* Recuperado de https://datasociety.net/wp-content/uploads/2018/10/DataSociety_Governing_Artificial_Intelligence_Upholding_Human_Rights.pdf

El autor[1034] señala que los *derechos humanos* pueden servir como una guía para el desarrollo y la gobernanza de la inteligencia artificial. Como recomendaciones iniciales se plantean algunas como las siguientes:

- "Las empresas tecnológicas deberían encontrar *canales efectivos de comunicación* con grupos de la sociedad civil local e investigadores a fin de identificar y responder a los riesgos". La interacción entre los actores y participantes del ecosistema de salud y *stakeholders* es imprescindible y necesaria.
- "Dado que los principios de derechos humanos no se escribieron como especificaciones técnicas, los abogados de derechos humanos, los encargados de formular políticas, los científicos sociales, los informáticos y los ingenieros deberían trabajar juntos en modelos de negocios, flujos de trabajo y diseño de productos**."**
- "Las compañías de tecnología e investigadores deben realizar *evaluaciones de impacto en los derechos humanos (EIRH)* a lo largo del ciclo de vida de sus sistemas de inteligencia artificial". En materia de protección de datos se trataría de un instrumento a desarrollar que ya existen como son las EIPD o evaluaciones de impacto del RGPD.

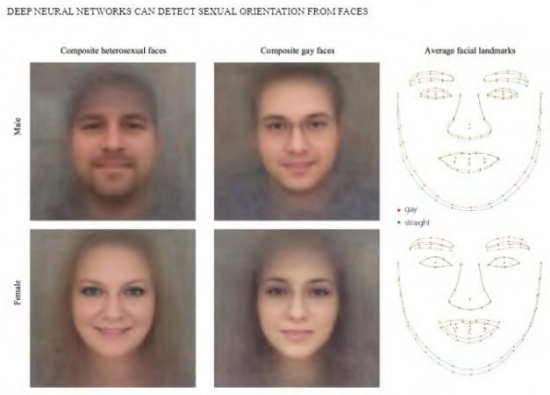


Imagen 78. Imágenes del estudio donde se contemplan posibles vulneraciones a la protección de datos por la orientación sexual.[1035].

Es especialmente preocupante sobre todo para los individuos y grupos en riesgo que son susceptibles de discriminación o estigmatización social, además de estar hablando de datos de orientación sexual como datos de categoría especial.

Hablemos de otro ejemplo.

Los sistemas de visión artificial confunden a personas de color con animales como gorilas[1036]. Es curioso también que, y como se ha estudiado[1037], los

[1034] *Ibídem.* Pp. 13
[1035] Vid. https://psyarxiv.com/hv28a/ pp. 22
[1036] Vid. https://elpais.com/tecnologia/2018/01/14/actualidad/1515955554_803955.html

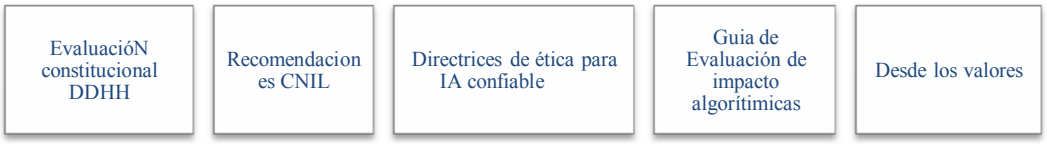
desarrolladores e innovadores suelen ser hombres blancos y de familias acomodadas. Lo más preocupante es que las máquinas terminan siendo una *caja negra* (*"black box"*, ver capítulo 2), opaca y llena de secretos, sin tener en cuenta su funcionamiento interno, incluso para sus propios desarrolladores. La forma de solucionar el problema es borrar el problema: autocensurar esas etiquetas.

Imagen 79. Ejemplo de black box y discriminación por raza. Fuente: El país

Y es que en 2017, pasó algo que se predecía, nos acercamos a la "Era de la *Singularidad"* [1038]; Facebook desconectó dos robots de conversación que habían desarrollado un lenguaje secreto sin que lo supieran sus desarrolladores. Ellos consideran que se trató de un error de programación porque ninguna máquina tiene intenciones ni las tendrá puesto que no tienen compasión ni sabiduría.

Parece obvio que los códigos éticos no son suficientes sino van acompañados de supervisión y responsabilidad para respaldar los compromisos éticos. Entonces, *¿cómo hacer responsables a los que no son responsables?*

2.3.2. Posibles soluciones y herramientas



i. *Realizar una posible "evaluación constitucional del sistema IA (desde la perspectiva de los DDHH)".*

[1037] Alex Bell & Raj Chetty & Xavier Jaravel & Neviana Petkova & John Van Reenen, 2019. "Who Becomes an Inventor in America? The Importance of Exposure to Innovation*," The Quarterly Journal of Economics, vol 134(2), pages 647-713. Recuperado de https://www.nber.org/papers/w24062

[1038] Vid. https://www.wired.com/story/facebooks-chatbots-will-not-take-over-the-world/

Philip Alston, profesor de Derecho Internacional de la Facultad de Derecho en la Universidad de Nueva York, propone una solución para la naturaleza ambigua e incomprensible de la ética: replantear las consecuencias impulsadas por la inteligencia artificial *en términos de derechos humanos*. Afirmó que **si** un sistema de inteligencia artificial elimina los derechos básicos de las personas, entonces no debería ser aceptable**.**

ii. Seguir las recomendaciones de la CNIL[1039]

a. Fomentar la educación de todos los jugadores.
b. Haciendo comprensibles los sistemas algorítmicos
c. Mejora del diseño del sistema algorítmico para evitar el efecto de "caja negra"
d. Creación de una plataforma nacional para auditar algoritmos;
e. Incentivos crecientes para la investigación en IA ética.
f. Refuerzo de la ética en las empresas mediante la creación de comités de ética, la difusión de buenas prácticas en cada sector o la revisión de códigos de ética.

Para el *Thing do tank Data Ethics*[1040], "las recomendaciones son todas muy relevantes y necesarias y se ajusta a nuestros principios y directrices de ética de datos, sin embargo, hay aún más discusiones que tomar.

a. *Función analógica*. En caso de que decidamos que todos los gadgets de IoT deben funcionar sin estar en línea. Cuando compre una máquina de café, ¿no debería estar funcionando sin estar en línea? ¿Es esta una demanda realista?
b. *Ayudar a fomentar y preservar un mercado de productos analógicos*. También podemos decidir que debemos poder comprar productos y servicios, que son análogos y que no solo deben ser asequibles para los ricos. ¿Podemos comprar una máquina de café en el futuro que no nos rastree a través de chips o sensores? ¿O comprar un auto donde subimos las ventanas y cerramos las puertas de nuestros autos con la mano humana?
c. *Botón de anulación manual* . Si permitimos el desarrollo de nuevos productos y servicios que dependen de Internet, al menos deberíamos exigir un 'botón de anulación manual' integrado. Con eso, un ser humano puede detenerlo, si la máquina funciona como loca. Si hubiéramos entendido lo que hacía *Google Search* cuando comenzó a personalizar las búsquedas, también podríamos

[1039] CNIL. (26 de diciembre de 2017). How can humans keep the upper hand? Report on the ethical matters raised by algorithms and artificial intelligence. Recuperado de https://www.cnil.fr/en/how-can-humans-keep-upper-hand-report-ethical-matters-raised-algorithms-and-artificial-intelligence

[1040] Tranberg, P. (19 octubre de 2018). Debating ethics: We need a "manual override" button. *DataEthics.* Recuperado de https://dataethics.eu/en/debating-ethics-we-need-manual-override/

haber exigido un botón rojo que neutralizó las búsquedas para no depender de quién eres y de lo que has hecho en el pasado.

d. *Privacidad por diseño.* Aunque el Reglamento de protección de datos general europeo, GDPR, promueve el uso de Privacidad por diseño, no es obligatorio y todavía estamos viendo la mayoría de los servicios y productos, que no son privacidad por diseño, ya que todavía no puede realizar el seguimiento. Necesitamos aplicar al menos la privacidad por defecto (uno de los criterios en Privacidad por diseño) en todos los dispositivos y servicios en el futuro, ya que exige a todos los seres humanos que piensen dos veces en sus propias responsabilidades y acciones sobre sus datos.

e. Debemos preguntarnos, si todo realmente necesita estar en línea y estar basado en datos. ¿Es necesario con un control remoto de su máquina de café o puede caminar hasta la máquina de café y esperar esos minutos mientras se prepara el café? ¿O necesita un dispositivo en la habitación para bebés que pueda reproducir una canción de cuna para su bebé, si se despierta y llora? Si solo escuchamos a la industria de la tecnología produciendo nuevos productos convenientes, terminaremos como adictos a la cama con un control remoto en nuestras manos."

iii. Seguir las recomendaciones del las *Directrices de ética para IA confiable ("Ethics Guidelines for trustworthy AI",* en versión borrador[1041]*,)* por el grupo de trabajo de alto nivel en IA.

Para el grupo de expertos, "la *IA confiable* tiene dos componentes: debe respetar los derechos fundamentales, las regulaciones aplicables y principios fundamentales, asegurando el "propósito ético; y debe ser técnicamente robusto y confiable" [1042].

[1041] Comisión Europea (19 de diciembre de 2018). Draft Ethics Guidelines for Trustworthy AI. Recuperado de https://ec.europa.eu/knowledge4policy/publication/draft-ethics-guidelines-trustworthy-ai_en. Ver también versión definitiva: https://us18.campaign-archive.com/?u=a23897532dbb6100934258190&id=803e0320a1 . Además, el 26 de Junio de 2019 se publica *un checklist* de ética para inteligencia artificial confiable. Recuerado de: https://ec.europa.ey/digital-single-market/en/news/eu-artificial-intelligence-ethics-checklist-ready-testing-new-policy-recommendations-are

[1042] Me parece conveniente sobre todo centrarnos en los requisitos y métodos de la IA confiable que se señalan en el borrador. (i) *Respecto privacidad.* La privacidad y protección de datos deben estar garantizadas en todas las etapas del ciclo de vida del sistema IA. Esto incluye todos los datos proporcionados por el usuario, pero también toda la información generada sobre el usuario a lo largo de su curso interacciones con el sistema IA. Los registros digitales del comportamiento humano pueden revelar altamente datos sensibles (como son los datos de salud). Señala algunos interrogantes como: Si corresponde, ¿es compatible el sistema con el RGPD? ¿está el flujo de información de datos personales en el sistema bajo control y cumple con las leyes de protección de la privacidad existente? ¿cómo pueden los usuarios buscar información sobre un consentimiento válido y cómo se puede revocar dicho consentimiento? ¿Está claro, y se comunica claramente, a quién o a qué grupo de cuestiones relacionadas con la violación de la privacidad pueden ser aumentadas, especialmente cuando estas pueden aumentarse por usuarios del sistema de IA u otros afectados por el mismo? (ii) *"Rendición de cuentas.* Dependerá de la naturaleza y el peso de la actividad. Puede incluirse mecanismos de compensación monetaria (sin culpa o con culpa) o conciliación sin compensaciones. Por ejemplo, un sistema IA que malinterpreta un medicamento y decide no reembolsar puede ser compensado monetariamente, sin embargo, si se tratara

Es de destacar los siguientes *métodos* para conseguir una IA confiable:

a. *"Métodos Técnicos:*
   - *Ética y estado de derecho por diseño* (*X-by-design*). La idea central es que el cumplimiento de la ley, así como de los valores éticos se pueden implementar, al menos en cierta medida, en el diseño del sistema AI.
   - *Arquitecturas para IA confiable.* Por ejemplo, por medio del monitoreo continuo.
   - *Pruebas y validación*.
   - *Trazabilidad y auditabilidad.* Para abordar los desafíos de la transparencia, los sistemas de IA *deben documentar* las decisiones que hacen y todo el proceso que dio lugar a las decisiones para tomar decisiones trazables.
   - *Explicación XAI.* Existe un problema conocido en los sistemas de aprendizaje basados en redes neuronales ("deep learning") y es la dificultad de proporcionar razones claras para la interpretaciones y decisiones del sistema. A veces pequeños cambios en los valores de los datos pueden derivar a cambios dramáticos y delicados en la interpretación (por ejemplo, personas de raza negra con animales). Existe un amplio campo de investigación abordando esta cuestión.

b. *"Métodos no técnicos:*

---

de una discriminación, serían necesarias explicaciones y disculpas. (iii) *Gobernanza de datos.* La calidad e integridad de los conjuntos de datos utilizados es primordial para el rendimiento del aprendizaje automático capacitado. (iv) *Diseño para todos.* Los sistemas deben diseñarse de una manera que permita a todos los ciudadanos utilizar los productos o servicios, independientemente de su edad, estado de discapacidad o estado social. permitiendo así el acceso equitativo y la anticipación activa de potencialmente todas las personas en actividades humanas existentes y emergentes. Este requisito enlaza a la Convención de las Naciones Unidas sobre los derechos de las personas con discapacidad. (v) *Gobernanza de autonomía de IA.* Cuanto mayor es el grado de autonomía que se otorga a un sistema de inteligencia artificial más exhaustivas serán las pruebas y el gobierno más estricto. La intervención humana será más o menos temprana en función de ello. (vi) *No discriminación.* La discriminación se refiere a la variabilidad de los resultados de la IA entre individuos o grupos de personas según la explotación de las diferencias en sus características que pueden considerarse intencionalmente o involuntariamente (como el origen étnico, el género, la orientación sexual o la edad), lo que puede tener un impacto negativo en tales individuos o grupos. El daño intencional puede resultar atan intencionalmente algoritmos para excluir a ciertos grupos. Por ejemplo, pensemos en las aseguradoras de salud que excluyen a grupos de personas con tendencias a enfermedades. Pero hay que tener en cuenta algo importante: la propia IA puede ayudarnos a identificar el propio sesgo inherente y ayudarnos a tomar las decisiones menos sesgadas. (vi) *Respeto (y mejora de) la autonomía humana.* Cada vez más los productos y servicios de IA se enfocan a personalizaciones "extremas" y a guían a las personas a elecciones potencialmente manipuladoras. Además, los individuos cada vez están más dispuestos a delegar decisiones y acciones a máquinas, pensemos, por ejemplo, en los asistentes personales como Alexa. (vii) *Robustez.* La IA confiable requiere que los algoritmos sean seguros, confiables y lo suficientemente robustos para lidiar con errores o inconsistencias durante la fase de diseño, desarrollo, ejecución, despliegue y uso del sistema AI, y para hacer frente adecuadamente a los resultados erróneos. (viii) *Seguridad. C*onsiste en garantizar que el sistema haga lo que se supone que debe hacer, sin dañar a los usuarios, recursos o medio ambiente. (ix) *Transparencia.* Conlleva a la capacidad de describir, inspeccionar y reproducir los mecanismos a través de los cuales los sistemas de IA hacen decisiones y aprenden a adaptarse a sus entornos, así como a la procedencia y dinámica de los datos que se utilizan. Se deben requerir fuentes, procesos de desarrollo y partes interesadas de todos los modelos que utilizan datos humanos o afectar a los seres humanos o puede tener otro impacto moralmente significativo".

- *Regulación*[1043]. Hoy existen muchas regulaciones que aumentan la confianza de IA como son la legislación de seguridad o la de responsabilidad civil. Saber que la reparación es posible cuando las cosas van mal aumenta la confianza. Los mecanismos pueden ir desde la compensación monetaria, negligencia o mecanismos de responsabilidad basados en la culpabilidad, la reconciliación, la rectificación y la disculpa sin la necesidad de compensación monetaria.
- *Estandarización.* El uso de estándares acordados para el diseño, la fabricación y las prácticas comerciales puede funcionar como un sistema de *gestión de calidad* para IA a los consumidores, actores y gobiernos. Más allá de los estándares convencionales existen sistemas de acreditación, códigos de ética profesional o estándares de derechos fundamentales. Algunos ejemplos son los estándares ISO.
- *Gobernanza rendición de cuentas.* Las organizaciones deben establecer un marco de gobierno interno o externo para garantizar la responsabilidad. Esta puede, por ejemplo, incluir el nombramiento de una persona a cargo de cuestiones de ética en relación con AI, una junta de ética interna, y / o una junta de ética externa. Esto puede ser adicional a, y no puede reemplazar, la supervisión legal; por ejemplo, en forma de DPO o equivalente.
- *Códigos de conducta.* Las organizaciones y las partes interesadas pueden suscribirse a las pautas y adaptar sus estatutos corporativos.
- *Educación.* Aquí se refiere a las personas que fabrican los productos (los diseñadores y desarrolladores), los usuarios (empresas o individuos) y otros grupos afectados.
- *Dialogo stakeholders.* Esto requiere un *debate abierto y la participación de los interlocutores sociales, partes interesadas y público en general*. Los paneles incluyen diferentes expertos y partes interesadas como expertos legales, técnicos expertos, especialistas en ética, representantes de los clientes y empleados, etc. Se buscará activamente la participación y el diálogo sobre el uso y el impacto de la IA apoyando la evaluación y revisión de los resultados y sus enfoques, incluyendo los casos complejos. Prueba de ello es el grupo de Alianza Europea de IA[1044].
- *Equipos con diversidad e inclusivos.* Esto contribuye a la objetividad y consideración de diferentes perspectivas, necesidades y objetivos. No solo es necesario que los equipos sean diversos en términos de género, cultura, edad, sino también en términos de experiencia profesional y habilidades".

iv. Siguiendo la Guia de Evaluación de impacto algorítimicas (AIAs)[1045].

[1043] El grupo de expertos considera que la regulación puede necesitar ser revisada, adaptada o introducida, hechos que serán discutido en el segundo entregable del borrador (marzo 2019) y que contarán con la colaboración de los 900 miembros de Alianza Europea de la IA.

[1044] Comisión Europea. The European AI Alliance. Recuperado de https://ec.europa.eu/digital-single-market/en/european-ai-alliance

[1045] Reisman, D., Schultz, J., Crawford, K., Whittaker M. (abril 2018). Algorithmic Impact Assesments: A practica framework for public Agency Accountability. *AINow.* Recuperado de https://ainowinstitute.org/aiareport2018.pdf

Dada la magnitud y el impacto ético que conlleva esta tecnología, parece necesario abrir el campo de visión y ampliar intervención por parte de las AAPP en su papel de supervisor, evaluador y controlador respecto a los sistemas de IA y de los actores intervinientes que pueden repercutir en los ciudadanos, garantizando el *principio de accountability y la due diligence públicos,* algo que no sólo debe importar u ocupar a EEUU[1046] o Canadá[1047].

Ahora bien, ¿por qué no extender la obligatoriedad de una AIA también en el sector público, para organizaciones?

Partimos de la base de que, como venimos defendiendo, las organizaciones tecnológicas, desarrolladores e ingenieros "deben abrir sus diseños al *control democrático*" (Joiito, 2018)[1048]. "Antes de obtener un nuevo sistema de decisión automatizado, las agencias tendrían que *divulgar públicamente información* sobre el propósito, alcance y posible impacto del sistema en las clases de personas legalmente protegidas"[10491050].

(¿Cuándo serán las decisiones automatizadas responsables por parte de las agencias públicas u organismos públicos? ¿cómo garantizar que apliquen el principio de accountability? ¿en que marco práctico se deben apoyar? O en definitiva, ¿quién controla al controlador?)

[1046] Vid. https://www.aclu.org/issues/privacy-technology/surveillance-technologies/algorithms-are-making-government-decisions

[1047] Vid. https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf

[1048] Vid. https://www.aclu.org/issues/privacy-technology/surveillance-technologies/ai-engineers-must-open-their-designs-democratic?redirect=issues/privacy-technology/consumer-privacy/ai-engineers-must-open-their-designs-democratic-control

[1049] Vid. https://www.aclu.org/issues/privacy-technology/surveillance-technologies/algorithms-are-making-government-decisions

[1050] Por tanto, "las agencias tendrían que respetar el *derecho del público al debido proceso,* es decir, garantizar que la participación pública significativa se integre en todas las etapas del proceso de AIA antes, durante y después de la evaluación a través de un proceso de *notificación y comentarios,* a través del cual las agencias solicitan la opinión pública sobre sus evaluaciones. Esta sería una oportunidad para que el público exprese sus inquietudes y, en algunos casos, incluso cuestione si una agencia debería adoptar un sistema de decisiones automatizado en particular. Además, si una agencia no completa adecuadamente un AIA, o si los daños no son resueltos por la agencia, el público debe tener algún método de recurso (o impugnación)". Ahora bien, llegados a este punto, el *AI Now Institute* se cuestiona; "¿cómo deberían financiarse los investigadores externos por sus esfuerzos? ¿Y qué deberían hacer las agencias cuando los proveedores privados que venden sistemas de decisión automatizados se resisten a la transparencia?". Según ellos "los proveedores deben ser obligados a renunciar a sus reclamos de secreto comercial sobre la información requerida para ejercer la supervisión". Pero, dicho esto y sin desentendernos de la visión jurídica, cabe preguntarnos *¿qué naturaleza podrían tener estas AIAs respecto a protección de datos y privacidad? ¿qué tiene que ver con el RGPD? ¿las AIAs se adaptarían a nuestra normativa comunitaria?* Según esta guía, "las evaluaciones de impacto algorítmicas se basan directamente en marcos de evaluación de impacto en la protección del medio ambiente, la protección de datos, la privacidad y los derechos humanos". Sin embargo, las PIAs de nuestro RGPD europeo se aplican tanto a organizaciones públicas como privadas, "*no son compartidas con el público, y no tienen una revisión externa incorporada por parte de un investigador".*

v. Desde los valores.

Eliezer Yudkowsky (2008) [1051] propone diseñar una IA amigable donde *"valores de tolerancia y respeto por el bienestar de los seres humanos* sean incorporados como elementos nucleares en la programación de agentes de IA".

2.4. Implicaciones éticas con IoT[1052] y m-Health.

Tenemos que asimilar que estos dispositivos cuantificadores van a jugar un papel importante como generadores de datos en el cuidado de la salud en el futuro, tanto a nivel clínico o de investigación, como de aseguradoras (Dans, 2018)[1053]. Así por

---

Según el IA Now, "el lenguaje RGPD puede ser un buen punto de partida, pero requerirá cierta configuración para coincidir con los contextos apropiados". (i) En primer lugar, algunas herramientas de vigilancia predictiva, por ejemplo, no necesariamente constituyen *"perfiles de individuos"* y, en cambio, se centran en ubicaciones, utilizando estadísticas para tratar de comprender. Una definición podría ser "cualquier sistema, herramienta o algoritmo que intente predecir las tendencias delictivas y recomendar la asignación de recursos de vigilancia *en términos no individualizados*. En general, cualquier definición debe asegurarse de cubrir sistemas que puedan *tener un impacto dispar en comunidades vulnerables"*. (ii) En segundo lugar, respecto al art. 22 RGPD (derecho a no ser objeto de decisiones basadas *únicamente* por procesamiento automatizado), opinan que "introduce un vacío legal para los sistemas que tienen algún grado de intervención humana. El GT29 en sus directrices[1050], "han intentado ajustarse a esto al exigir que la *intervención humana sea significativa* en lugar de un *gesto simbólico* y que los responsables de datos discutan la participación humana en sus evaluaciones de impacto de protección de datos".

[1051] *Supra Cit.*

[1052] Quizás podríamos utilizar la clasificación de las tres áreas de reflexión ética que ocupa a la IoT que bien señala la autora Colmenarejo (2017): (i) *"La ciberética*; que se ocupa de analizar los modos en los que internet está condicionando la comunicación social entre individuos y organizaciones. (En este se podría incluir la ética de IoT e incluso la ética de la robótica donde se han identificado valores negativos como la vigilancia masiva). (ii) *La ética de la computación;* comparte espacios con la ciberética, en tanto que se ocupa de la tecnología que se emplea para la recopilación, gestión y tratamiento de los datos, pero sin ceñirse a internet, es decir, se ocupa de los problemas éticos que surgen en el desarrollo y utilización de herramientas computacionales en todos los ámbitos de la sociedad (Johnson, Miller, 2009; Stahl et al, 2016). (iii) *La ética de la información en investigación biomédica como parte de la bioética* que se ocupa de analizar la interacción entre seres vivos y tecnologías digitales y/o computacionales, pero sin ceñirse únicamente a la obtención y gestión de datos obtenidos mediante un acto médico, sino también de los biométricos obtenidos con fines de vigilancia y seguridad (Bietz et al., 2016; Kokumi, 2016; Sharon, 2016; Stylianou, Talias, 2017)".

[1053] Por otro lado, según Dans (2018) compañías como "Nest (Alphabet) han llevado recientemente a cabo adquisiciones como Senosis (spinoff de la Universidad de Washinngton) dedicada al desarrollo de sistemas de monitorización de salud mediante el smartphine y dejan claras las intenciones de custodia de datos y registros médicos". O, Apple que presentó una API para que los desarrolladores de apps pudieran trabajar con datos almacenados en su aplicación, para que con el nivel adecuado, compartieran esos datos con distintos proveedores de salud : médicos, hospitales, investigadores médicos, etc para recibir recordatorios y mejorar la adherencia a tratamientos, etc**.** Esta integración continúa con el compromiso de Apple de proporcionar a la comunidad médica herramientas de ResearchKit que podrían promover sus descubrimientos. Para más info: https://9to5mac.com/2018/06/04/apple-opens-health-records-api-for-developers/

ejemplo, *Apple Watch serie 4*[1054] en la actualidad ya cuenta con un sensor que permite hacer electrocardiogramas**.** Y es que de acuerdo con un informe de la Universidad de California**,** el *Apple Watch* es capaz de detectar arritmias cardíacas con una exactitud del 97 %**,** por lo que se trata de un buen dispositivo para personas que puedan sufrir problemas del corazón. Este dispositivo ya ha podido salvar la vida a más de una persona[1055] [1056]**.**

No podemos desconocer los grandes avances que esta tecnología pueden traer a los usuarios en el futuro, ahora bien, sin pretender ser una barrera a la innovación y a los avances tecnológicos -ni mucho menos-, tenemos que estar atentos algo muy importante: la privacidad, protección de datos y la ética de los datos de los dispositivos de salud IoT.

La mayoría de los *rastreadores de fitness*, por ejemplo, pierden datos personales y no son seguros para la privacidad[1057].

En el 2015, en alguna encuesta[1058], ya las aseguradoras (51%) querían asociarse con grandes empresas de tecnología digital y plataformas cloud, quedando evidente la tendencia y la intención de la industria. Los usuarios que participan aportando datos a

---

[1054]Vid.https://www.revistagq.com/noticias/tecnologia/articulos/apple-watch-series-4-critica-caracteristicas-opiniones/30946 . Este dispositivo cuenta con el certificado de la FDA estadounidense (aunque la AME europea no lo ha otorgado por el momento**),** lo que significa que le ha otorgado la misma validez para hacer electrocardiogramas tan como lo hacen otros aparatos. Este dispositivo permitirá registrar, por ejemplo, una arritmia del usuario para que posteriormente pueda mostrársela al médico. Otra de las opciones que tiene el dispositivo es el detector de caídas que posibilitaría una llamada a los servicios de emergencia si no es capaz de responder. Este servicio se activará automáticamente cuando el usuario tenga 65 años o más, de lo contrario se activa manualmente**.**

[1055] Vid. https://www.tribuna.com.mx/cienciaytecnologia/Nueva-herramienta-en-el-Apple-Watch-salva-la-vida-de-una-persona-20181209-0083.html

[1056] Vid. https://elchapuzasinformatico.com/2018/05/un-apple-watch-salva-la-vida-a-un-hombre-tras-detectar-una-ulcera-perforada/ En uno de los casos, un usuario pudo salvar su vida gracias a la alerta que le emitió cuando el ritmo cardiaco no era el normal. Este usuario empezó a sangrar en el trayecto de la ambulancia hasta el punto de perder el 80% de su sangre. Según el grupo médico, sin este dispositivo el usuario no se habría percatado con el suficiente tiempo de que algo iba mal para salvar su vida.

[1057] Una investigación de la Universidad de Toronto ha analizado a *Apple Watch, Basis Peak, Fitbit Charge HR, Garmin Vivosmart, Jawbone Up 2, Whitings Pulse O2, Mio F use y Xiaomi Mi Band* y ha concluido que 7 de cada 8 (salvo *Apple*) emiten identificadores únicos persistentes que pueden exponer a los usuarios aun seguimiento a largo plazo sobre su *ubicación* cuando el dispositivo está conectado a un móvil A su vez, las aplicaciones *Garmin Connect* (*iPhone y Android*) y la aplicación *Withings Health Mate* (Android) tienen vulnerabilidades de seguridad que permiten a un tercero no autorizado leer, escribir y eliminar datos de usuarios. Para más info: https://dataethics.eu/en/fitnesstrackersleak/. Las consecuencias éticas no sólo estarán al torno de la "*fatiga de hiperconectividad"* que puede suponer estar conectado a estos dispositivos sino también al impacto de esta tecnología sobre la privacidad e intimidad de los usuarios.

[1058]Vid. https://www.ituser.es/movilidad/2015/05/el-31-de-las-aseguradoras-utiliza-wearables-para-comunicarse-con-clientes-empleados-y-socios

las aseguradoras obtienen descuentos premium por alcanzar objetivos de ejercicio. Surgen varios interrogantes: ¿Las aseguradoras de "seguros de vida interactivos" [10591060] podrán usar los datos para seleccionar a los clientes más rentables mientras que las tasas de interés aumentan para aquellos que no participan? ¿las aseguradoras pueden crear perfiles de clientes menos rentables?¿qué podrían hacer las personas que se le niegan o cancelan un seguro de vida porque los hábitos no están considerados de saludables? ¿es justo pagar más en la póliza de esas aseguradoras por no querer enviar datos de salud o dejarse monitorizar por dispositivos de IoT de salud? ¿cómo poner control ético de los datos a la sociedad hiperconectada en la que vivimos? ¿qué información debe liberarse a la red pública sobre los pacientes?

También se despiertan dilemas éticos en los "hospitales conectados" con IoT debido a las vulnerabilidades de seguridad de los mismos dispositivos sobre todo en los hospitales norteamericanos[1061].

Otra cuestión inquietante la ocupa las vulnerabilidades de los marcapasos. Según una encuesta de la AERC[1062], la monitorización remota está disponible para el 22% de los pacientes con marcapasos. Para la investigadora *Carmen Cámara,* "el sistema se vuelve inseguro y surgen las mismas amenazas que se dan en dispositivos informáticos comunes como un PC o un móvil, pero con consecuencias más graves". Esta situación empezó a preocupar tanto que, por ejemplo, el vicepresidente de EEUU de aquel entonces, desactivó la función inalámbrica de su propio marcapasos[1063].

[1059] Vid. https://www.reuters.com/article/us-manulife-financi-john-hancock-lifeins/strap-on-the-fitbit-john-hancock-to-sell-only-interactive-life-insurance-idUSKCN1LZ1WL

[1060] También las aseguradoras de salud han sufrido de ataques ciberdelincuentes como fue el caso de Anthem, afectando a 80 millones de personas. Vid.http://www.forbes.com/sites/brucejapsen/2015/02/08/anthem-cyber-attack-clouds-insurers-obamacare-bounty/

[1061] Han aumentado un 125% y cuestan 6.000 millones de dólares al Sistema de Salud[1061]. Por ejemplo, en el 2014 se produjo en EEUU un robo masivo de 4,5 millones de pacientes con datos personales de número de seguridad social, nombres, direcciones, teléfonos y fechas de nacimiento de los pacientes. La intención de los hackers en este caso no era la información personal sino la propiedad intelectual almacenada en los dispositivos. Las consecuencias son la pérdida los HCE (pueden hacer que los médicos realicen tratamientos equivocados poniendo en riesgo la vida de los pacientes), o el acceso de los propios dispositivos (bomba de insulina o respirador). En otros caso, el objetivo de estos incidentes es el robo de dinero o chantaje[1061]. Vid. http://www.techtimes.com/articles/69953/20150718/ucla-health-data-breach-affects-4-5-million-patients-what-you-should-know.html

[1062] Vid. https://www.ncbi.nlm.nih.gov/pubmed/25713012

[1063] Vid.https://www.researchgate.net/publication/275413868_Security_and_Privacy_Issues_in_Implantable_Medical_Devices_A_Comprehensive_Survey

Lo que es claro es que la ética aplicada a la *IoT de la salud y a m-Health*[1064][1065] deberá estar orientada a desarrollar una determinada *cultura ética de los datos* que permite tomar decisiones orientadas hacia el interés general de la sociedad o bien común, en general, y a la privacidad y protección de datos de las personas, en particular.

2.5. Implicaciones éticas con *Blockchain/DLT*.

Desde el punto de vista de la ética de los datos de las personas, en un contexto de la proliferación masiva de silos de bases de datos centralizados con información sensible de las personas, las virtudes de *blockchain* posibilitarán que los titulares de los datos personales tuvieran *control sobre sus datos* en diferentes formas.

Además, proporcionaría *valor* en la atención médica al permitir un *intercambio seguro* y específico de datos para mejorar la calidad y reducir el coste de la atención médica y habilitar nuevos sistemas de *comercio e incentivos*. Por ejemplo, los participantes (entidades de atención médica, pacientes[1066], etc.) que participan en una cadena de bloques pueden ser recompensados por el comportamiento deseado.

Desde el punto de las organizaciones privadas (o instituciones públicas), se concibe a este protocolo como una solución de *responsabilidad social empresarial* (RSE)[1067].

[1064] Hablemos de un ejemplo de problema ético en eHealth y menores de edad. La Dra. Kressly, pediatra de Warrington en la Conferencia Anual de la Sociedad de Sistemas de Información y Gestión de la Salud (HIMSS) en Las Vegas (2018) alarmó de la vulnerabilidad del derecho de protección de datos de los adolescentes donde propone a eHealth como solución (con una solución centrada en el paciente, capaz de ayudarlos donde están, y sea rápida, fácil y gratuita). Ponía el ejemplo de la adolescente que acude al médico para pedir la receta del día después. En el momento que se escriba la receta se enviarán los datos a los padres vulnerando el derecho fundamental de la menor. Esta doctora sugerió la implementación de estándares para los "roles" del personal (ej. cualquier miembro del personal, solo personal clínico, solo proveedores o solo médicos).

[1065] Vid. http://www.intotheminds.com/blog/en/30-days-to-read-privacy-policies-consent-fatigue-will-make-gdpr-ineffective/

[1066] En este sentido, merece especial atención a lo que pueda venir en el futuro respecto blockchain y RRSS (piénsese, en la moneda de FB, libra anunciado en el mes de junio de 2019), donde ya se han recibido numerosas críticas acerca de la falta de descentralización, en concreto, en los sistemas de SII o identitificación soberana, a las que añadiría implicaciones en protección de datos de los usuarios. Recuperado de https://www.technologyreview.es/s/11265/el-secreto-oculto-tras-el-anuncio-de-la-cadena-de-bloques-de-facebook

[1067] Ésta, desde el enfoque de la protección de datos y privacidad, se podría definir como la contribución activa y voluntaria al mejoramiento social que tiene por objetivo el de mejorar su situación competitiva y valorativa teniendo en cuenta el respeto del derecho fundamental de la protección de datos de los individuos. La RSE va más allá del mero cumplimiento de la normativa, por ejemplo, la RGPD. En este sentido, la CNIL francesa, en su *guía sobre blockchain y protección de datos*, recomendó a los actores

Blockchain o los sistemas DLT, como *protocolo*, permiten ciertas exigencias como la anonimización (medida técnica y organizativa que obliga la normativa) de la información almacenada sensible como es la de la salud. No obstante, no podemos desatender la idea de que *blockchain* tiene ciertas limitaciones (ej. derecho al olvido, minimización, etc.) Es aquí donde la RSE tendrá un papel muy importante que se traducirá en una contribución activa en la *"búsqueda creativa"* de técnicas y herramientas que posibiliten y den solución de alguna manera a las incompatibilidades de este protocolo con la normativa. Puede suponer todo un desafío para los desarrolladores quienes saben que en esa búsqueda pueden "desvirtuar" la tecnología.

2.6. Implicaciones éticas del futuro: neuroinformática, neurotecnología y biohacking, informática cuántica y genética.

2.6.1. Implicaciones éticas con neuroinformática.

La biometría es una técnica que vale tanto para la identificación como para la autenticación, y los datos registrados son datos personales que pueden vulnerar la privacidad de las personas por hackeos u otros[1068]. Hay investigadores[1069] que han explorado un modelo experimental *("Brain Password")* sistema biométrico cerebral cancelable como "sistema de autenticación móvil segura". En el futuro, este sistema permitiría desbloquear el móvil, abrir la puerta, con la mente (o algo parecido). Los creadores de este sistema aseguran que *"las credenciales criptográficas más seguras pueden obtenerse mediante ondas cerebrales de potencial relacionado con eventos".*

Consideran análogos una contraseña fuerte con números, letras y caracteres especiales con el diseño de nuestra contraseña cerebral que también incluye una mezcla de distintos estímulos visuales que fortalecen la contraseña.

---

que implantan proyectos tecnológicos, planteen el protocolo *blockchain* en lugar de otras alternativas tecnológicas.

[1068] En 2015 un *hacker* consiguió replicar el iris de Angela Merkel a partir de una foto. Vid: https://retina.elpais.com/retina/2017/07/04/tendencias/1499160204_361460.html

[1069] Lin, F. et al. (2018). Brain Password: A Secure and Truly Cancelable Brain Biometrics for Smart Headwear. *MobiSys '18*, June 10–15, Munich, Germany. Recuperado de http://cse.ucdenver.edu/~linfen/papers/2018_Mobisys_Brain_Password.pdf

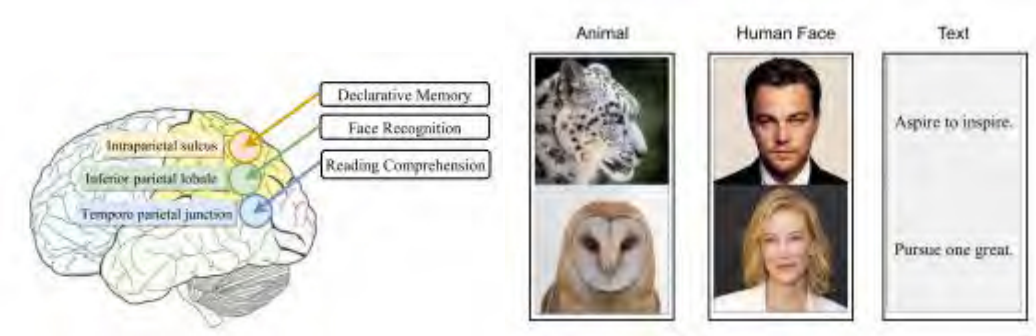


Imagen 80. Brain Password. Fuente: UCDenver.

En el modelo, los investigadores seleccionan imágenes de un animal, un famoso humano y un segmento de texto como estímulos para las áreas que procesan la memoria declarativa, el reconocimiento facial[1070] y la comprensión lectora, respectivamente.

Ya de por sí, no nos cuesta entender que no serán pocos los riesgos éticos en el ámbito de la privacidad que pueden acarrear, por ejemplo, un ataque de ciberseguridad a los datos personales de nuestras huellas digitales[1071] o de nuestro iris, que funcionan como sistemas biométricos de reconocimiento integrados en dispositivos. No nos constará trabajo imaginar las consecuencias que puede tener un "hackeo de contraseña mental"[1072].

2.6.2. Implicaciones éticas con neurotecnologías y el biohacking.

[1070] Vid. Tran, Dat. (2 de julio 2019). Paying in China CN these days: no card, no phone, only your face is enough. (Actualización de Twitter) Recuperado de: https://www.linkedin.com/feed/update/urn:li:activity:6551721808855343104/

[1071] Ver https://www.linkedin.com/feed/update/urn:li:activity:6521620270313275392/. *Nicola Vanin* señaló : "Existe un mercado de delitos cibernéticos en el que se venden hashtags# huellas dactilares completas para más de 60,000 usuarios. Este nuevo servicio no se parece a nada que se haya visto hasta ahora en la escena del crimen cibernético. El producto principal está representado por los perfiles digitales completos de los usuarios. Cada perfil de usuario incluye credenciales de inicio de sesión para cuentas en portales de pago en línea, servicios de banca electrónica, servicios de intercambio de archivos o hashtag# socialnetwork , pero también cookies asociadas con esas cuentas, detalles del agente de usuario del navegador, firmas de hashtag WebGL. # huellas dactilaresLienzo HTML5 y otros detalles del navegador y PC. Esta información se vende a otros grupos cibercriminales. La principal clientela del mercado son los delincuentes cibernéticos involucrados en el fraude en línea, el robo de identidad y las operaciones de mulas de dinero. Los creadores de este nuevo comercio han examinado 47 de los mejores sistemas de defensa analítica y 283 bancos para brindarle la combinación más eficiente para evitar sus sistemas de protección."

[1072] El problema se podría solucionar modificando los estímulos con nuevas imágenes y texto, por lo que "no necesitaríamos otro dedo o cerebro".

¿Qué consecuencias podría tener que los cerebros pudieran estar conectados entre sí para la privacidad "mental"? ¿o que se pudiera acceder a la información (y robarla) de un cerebro e insertar información o manipular? En una línea parecida, investigadores japoneses están diseñando una red neuronal ("*deep learning*") para que smartphones puedan leer mentes mediante el escaneo de las ondas cerebrales dentro de cinco años[1073].

2.6.3. Implicaciones éticas con la informática cuántica[1074].

Muchos investigadores predicen la peligrosidad de la llegada de la informática cuántica que podría suponer el fin de la privacidad[1075]. Los ordenadores cuánticos por su naturaleza técnica (la cual no vamos a entrar ahora) podrán ser descifradas instantáneamente las claves de nuestro correo electrónico gmail en cuestión de segundos. Escalofriante, ¿verdad? En dos décadas posiblemente la seguridad y la privacidad estará en peligro. No obstante, para algunos expertos en la materia ya se "han desarrollado otros métodos de cifrado que no sabemos hackear, ni siquiera con ordenadores cuánticos. Eso sí, estos métodos son más costosos o complejos que los actuales. Cuando existan ordenadores cuánticos habrá algunos problemas prácticos que resolver para cambiar toda la infraestructura actual de internet a estos nuevos métodos" (Cirac, 2018) [1076]. En el futuro, estará en la encriptación cuántica, más bien. Respecto a su aplicación en las ciencias de la vida o la salud, el impacto puede ser muy grande. Por ejemplo, *Atos* y *Bayer* están trabajando juntos, utilizando datos reales anónimos tiene como objetivo analizar e identificar las correlaciones entre comorbilidades y patrones relevantes de desarrollo de la enfermedad. El concepto complementa el enfoque de los ensayos clínicos, que generalmente se centran en un número limitado de pacientes y datos bien estructurados para el análisis de los indicadores de la enfermedad. Ahora bien, la clave del futuro, en mi opinión será la combinación de IA y computación cuántica, aunque aún es un

[1073] The Futurist. (20 enero 2019). Japanese researchers are teaching mobile phones how to read minds by scanning brain waves!". Recuperado de https://twitter.com/thefuturist007/status/1087067132746219523?s=12

[1074] Vid. https://www.lavanguardia.com/tecnologia/20181011/452295053145/vida-artificial-computacion-cuantica-pais-vasco.html. Ver también : https://singularityhub.com/2019/02/26/quantum-computing-now-and-in-the-not-too-distant-future/

[1075] Vid. https://www.internautas.org/html/9927.html

[1076] Vid.https://www.abc.es/ciencia/abci-ignacio-cirac-estamos-puertas-segunda-revolucion-cuantica-201705052018_noticia.html

territorio nuevo[1077]. No obstante no podemos desdeñar las ventajas que otorgaría esta tecnología a la Medicina[1078]. Podrá permitir el desarrollo de medicamentos a medida, por ejemplo. La cuántica permite realizar varios cálculos o simulaciones de manera simultánea en lugar de secuencial, permitiendo diseñar nuevos medicamentos con los computadores de manera mucho más rápida y barata. En la actualidad, la creación de medicamentos implica años de experimentos de laboratorio.

2.6.4. Implicaciones éticas con la genética.

Por parte de las instituciones comunitarias, está clara la cuestión; "los aseguradores no deberían requerir pruebas genéticas para efectos del seguro. En conformidad con el principio establecido en el artículo 12 de la Convención de Derechos Humanos y la Biomedicina, los datos predictivos como resultado de las pruebas genéticas no deben ser procesados a efectos del seguro salvo que esté autorizado por la ley[1079]. Por otro lado, un equipo de científicos de la Universidad de Harvard consiguió hace un par de años insertar imágenes fijas y en movimiento en el ADN de bacterias de la especie *Escherichia coli*. Según un estudio[1080] publicado por *Nature,* ellos demostraron cómo codificar imágenes sustituyendo píxeles por nucleótidos de ADN que quedan integrados en el genoma de las bacterias y que posteriormente se recuperan con un 90 por ciento de su resolución original. Por tanto, en el futuro se podrá almacenar una foto o un gif[1081] en nuestros ADN como si de un pen drive se tratara. Esto es gracias a la técnica CRISPR y resulta totalmente revolucionario.

[1077] Vid. https://www.cio.de/a/quantum-learning-machine-analysiert-krankheitsbilder,3592071
[1078] Vid https://blogs.iadb.org/salud/es/tecnologias-cuanticas/?fbclid=IwAR3qOOmjmw7OSqTrpipx353wB97jgWdbbYjN2uB3eWv_m3_yVEmac59X56A
[1079] Ver principio 4, punto 15-16 de la Recomendación del Consejo de Europa.
[1080] Ver estudio aquí.
[1081] Ver gif aquí

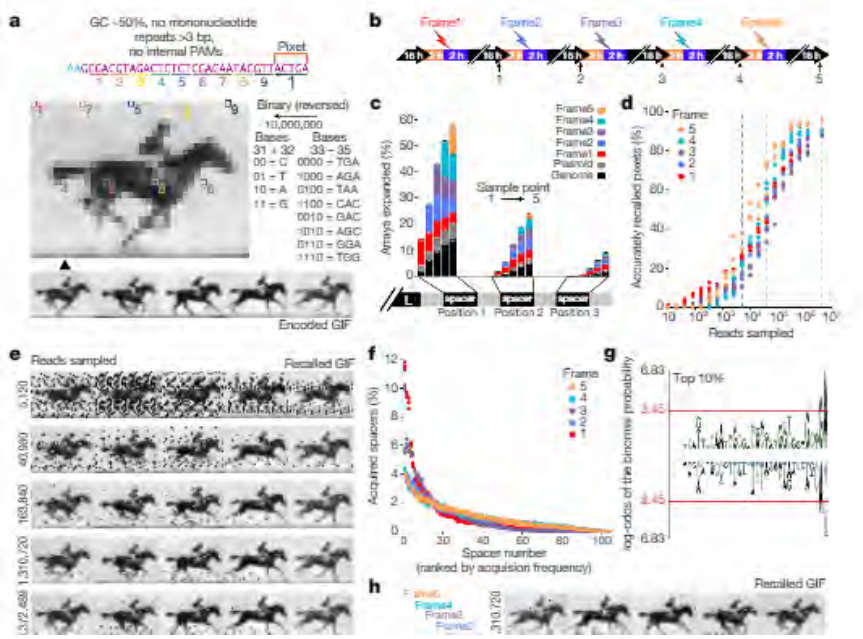


Imagen 81. Introducir datos en nuestro ADN como si fuera un pen drive. Fuente: Nature.

3. LA ETICA DE LOS DATOS Y LAS PERSONAS

"La tecnología está secuestrando nuestras mentes y la sociedad"

Tristan Harris, ex Filósofo Google (2017)

"Usted" fue elegido en el año 2006 como la "persona del año" en la revista *Time*[1082]. La revista se propuso reconocer a los millones de personas que contribuyen anónimamente con contenido generado por usuarios a wikis y otros sitios web como *Wikipedia, YouTube, MySpace, Facebook* y la multitud de otros sitios web que ofrecen contribuciones de usuarios.

[1082] Vid. http://content.time.com/time/specials/packages/0,28757,2019341,00.html

Imagen 82. Portada de la Revista Time Año 2006. Introducir datos en nuestro ADN como si fuera un pen drive. Fuente Wikipedia.

Pero como dicen no tardó en llegar la "*digital web 2.0 hangover*" (*Tranberg y Hasselbach*, pág. 17) o resaca digital, en castellano. La concienciación por la privacidad de nuestras identidades digitales y datos personales empezó a llegar. Posiblemente los individuos no pensaban que regalar los datos personales (sin consentimiento) fuera un problema si era para destinos específicos, pero la situación cambió cuando empezaron a entender que la combinación de esos datos con otros podrían derivar a perfilados y averiguar si una persona estaba embarazada, por ejemplo.

Ahora en la actualidad, en el 2019, nos podemos dar cuenta que "los individuos y los consumidores ya no están simplemente preocupados por la falta de control sobre sus datos personales sino que también están empezando a actuar en él y reaccionar con protestas, bloqueadores de anuncios y servicios encriptados (*Tranberg y Hasselbach, pág. 23*)[10831084].

[1083] Para Tranberg y Hasselbach, "los usuarios del motor de búsqueda anónimo *DuckDuckGo* aumentaron en un 50% en 2013, las herramientas de cifrado de *Silent Circle* crecieron un 400% en ventas semanales, mientras que el servicio en la nube encriptada de *Spider Oak* aumentó un 150%".

[1084] Esto tiene una traducción clara: este modelo de negocio se hunde, porque son los propios usuarios los que incluso quieren instalar bloqueadores de anuncios o proporcionar a los recolectores de datos, información falsa a modo de protesta. Hoy en día, tenemos menos control de los datos que forman nuestra identidad digital, como, por ejemplo, nuestras enfermedades, hábitos o necesidades y ha derivado a una preocupación social generalizada por la vigilancia digital. Es evidente que el grado de preocupación por la vigilancia digital de los gigantes tecnológicos varía geográficamente hablando. No es lo mismo la concienciación en Europa (vigilancia comercial privada) o EEUU (vigilancia pública del Gobierno) que en países de Oriente Medio donde la mayor preocupación es el acceso básico a Internet.

3.1. Preocupación por la privacidad.

"Renunciaremos a nuestra privacidad por una mejor salud"
HARARI

Especial preocupación despierta, desde mi punto de vista, la "falsa" impresión de obligatoriedad de cesión de datos personales por parte del paciente o usuario de servicios de salud sin la que no se podría acceder a la asistencia médica[1085].

Como mínimo, el proceso para obtener el consentimiento debe separarse del proceso para obtener la asistencia médica. Si no desea ceder su información de inmediato o tiene dudas sobre la seguridad de la recopilación de datos por parte de su médico**,** debería poder recibir la atención médica de todos modos" [1086] [1087].

¿Cuando hablamos de "empoderamiento individual" a qué nos referimos?

[1085] En este sentido, la socióloga e investigadora estadounidense *Mary Madden,* ha señalado en un artículo recientemente que "cuando optamos por no participar, **corremos el riesgo de perder el acceso a la asistencia médica que necesitamos".**

[1086] Vid. https://www.technologyreview.es/s/10632/riesgos-de-la-salud-20-si-quiere-ver-al-medico-debera-ceder-sus-datos

[1087] Por otro lado, las autoras *Tranberg y Hasselbach* (2018, 51-53) señalan varios casos simbólicos donde se puede apreciar que los usuarios prefieren pagar por tener privacidad según estudios realizados en el que participó el investigador italiano *Acquisti*. En uno de ellos (Vid. The Effect of Online Privacy Information on Purchasing Behaviour: An Experimental Study, Janice Tsai, Serge Egelman, Lorie Cranor, Allessandro Aquisti, Weis, 2007 https://www.econinfosec.org/archive/weis2007/papers/57.pdf) se pidió a los participantes que utilizaran un motor de búsqueda diseñado para comprar un paquete o juguetes sexuales con tarjetas de crédito. Cuando la búsqueda resultados sólo nombraba las tiendas en línea, los sujetos no estaban interesados en las políticas de privacidad y directamente compraban los productos más baratos. Pero si los resultados de la búsqueda también mostraban *información comprensible* sobre las diferencias en las políticas de protección de la privacidad de las tiendas online (por países), los participantes preferían pagar un 5% más para obtener el más alto nivel de privacidad. En otro, "los compradores de los grandes almacenes podían elegir entre recibir una tarjeta de regalo anónima con 10$ para compras y una tarjeta de regalo con 12 dólares que rastreaba las compras".
(Vid. What is privacy worth?, Alessandro Acquisti, Leslie John, George Loewenstein, The Journal of Legal Studies, Vol. 42, No. 2, The University Chicago Press, 2013. https://www.cmu.edu/dietrich/sds/docs/loewenstein/WhatPrivacyWorth.pdf).
Su conclusión fue que no hay evidencia que demuestre que a los consumidores generalmente no les importa sobre su privacidad. El valor que atribuyen a su privacidad es complejo y está sujeto a una variedad de factores, tales como sus motivaciones personales y la forma en que se les presentan las opciones. La observación de que los individuos dan su información personal por pequeñas recompensas ha permeado el debate político y se ha utilizado para argumentar en contra de la privacidad (por ejemplo, Rubin y Lenard 2002) sobre la base de que si los consumidores quisieran más privacidad, la pedirían y aprovecharían las oportunidades para protegerla.

3.1.1. ***Preocupación de los ciudadanos por la privacidad en general***

En *Europa*, la gran mayoría de los ciudadanos aceptan que los datos es parte del modelo de negocio digital y un prerrequisito para acceso a muchos productos y servicios digitales. El Eurobarómetro (2015)[1088] deduce en el apartado de conclusiones que "la mayoría de los encuestados aceptan que la recopilación de datos es parte en la vida moderna, siempre y cuando se mantenga dentro de los límites apropiados límites".

El *Eurobarómetro* señala lo siguiente;

- Respecto al *control individual* : sólo el 15 % de los encuestados sienten que lo tienen.
- Respecto a la *responsabilidad de la seguridad de la recogida*, intercambio y almacenamiento de datos: 67% (las empresas deberías ser los 1os responsables) y el 55% (las Aut. públicas deben ser los 1os responsables para garantizar).
- Respecto al *información de políticas de privacidad* : menos de una quinta parte de los encuestados admite que leen completamente las declaraciones. Aquellos encuestados que afirmaron no leerlas, dieron diferentes motivos: el 67 % se motivaron en la gran extensión de las mismas y el 38% lo justificó debido a la poca claridad o gran dificultad para entender las políticas de privacidad.

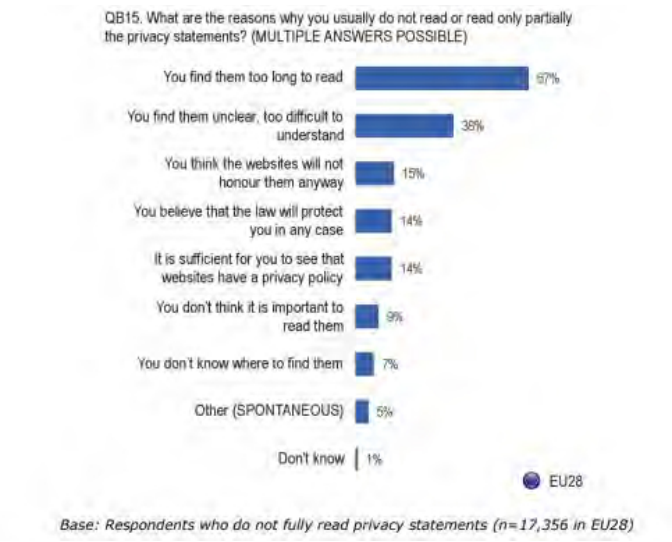


Imagen 83. Gráfico opiniones a la pregunta: ¿cuáles son las razones por las que normalmente no lees o lees solo parcialmente las políticas de privacidad?. Fuente: Comisión Europea. Special Eurobarometer 431.

- Respecto a los *riesgos*, lo que más les preocupa a los individuos encuestados es el fraude o el robo de identidad.

[1088] Vid. SEPD. (2015) Special Eurobarometer 431. Recuperado de http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_sum_en.pdf

En *España* según el CIS (2018)[1089], podemos extraer las siguientes conclusiones:

- Respecto a la *información de los riesgos* que supone proporcionar datos personales, el 36% señala estar poco informado y el 16% nada informado.
- Respecto a la imagen de *cultura de protección de datos* e implantación práctica, los encuestados valoran con mejor nota a las AAPP (Hacienda, SS, servicios sanitarios) y a los que califican con peor nota son a las RRSS y motores de búsqueda.
- Respecto a la *información de la políticas de privacidad*: el 33% de los encuestados respondió que nunca las lee.
- Respecto al *ejercicio de los derechos de los titulares* de datos personales (acceso, rectificación, cancelación, etc.…) solo el 26% lo ha ejercitado.
- Respecto al *spam publicitario*, el 68% señaló que recibió llamadas o mensajes recibiendo publicidad.
- Respecto a la *concienciación de la categoría especial de los datos personales* individuales, existe mayor preocupación por proporcionar datos personales con gustos y opiniones (40,4%), nombre y apellidos (36,9), su dirección (20,9%), historial laboral (26,2%), número de teléfono (15,7%) *historial clínico* (14,2%) (dolencias, enfermedades, etc.) y huellas dactilares (datos biométricos) (3,3 %).De aquí se deduce que no existe mucha concienciación acerca de la categoría especial de los datos de salud, un resultado que personalmente me ha sorprendido.
- Respecto a las *medidas sancionadoras*, la mayoría de los encuestados creen que imponer multas es la mejor medida para atacar las infracciones (48%), mucho mejor que la regulación o la educación en materia de protección de datos (cultura de privacidad) (5,4%).

El periodista, Tobias Stone[1090] en su artículo *"Su privacidad se ha terminado",* señala que "no estamos preparados como sociedad para el final de la privacidad y el armamento masivo de información, como lo han demostrado los últimos dos años".

1.1.2. Preocupación de los pacientes

Hemos hablado de los ciudadanos, hablemos de los pacientes; ¿cuál es su preocupación? ¿tienen reticencias en proporcionar sus datos personales de salud para investigaciones? En un informe de la Comisión Europea[1091] (2018) se analizaron los resultados de las una consulta realizada para la preparación de una Comunicación sobre la Transformación de la salud y la asistencia sanitaria en el mercado único digital. Con las siguientes conclusiones a destacar:

[1089] CIS. Barómetro de mayo 2018. Estudio n. 3213. Recuperado de http://datos.cis.es/pdf/Es3213mar_A.pdf

[1090] Vid. https://medium.com/s/story/your-privacy-is-over-ed72d06418f1

[1091] Comisión Europea. (2018). Consultation: Transformation Health and Care in the Digital Single Market. Recuperado de https://ec.europa.eu/health/sites/health/files/ehealth/docs/2018_consultation_dsm_en.pdf

- Más del 93% de los encuestados en línea creen que los ciudadanos deberían ser capaces de *gestionar sus datos de salud.*
- El 81% de los encuestados cree que compartir datos de salud podría ser beneficioso para mejorar el tratamiento, el diagnóstico y la prevención de las enfermedades en toda la UE.
- El 64% de los *stakeholders* y ciudadanos encuestados expresaron que debería haber una oportunidad de *optar por no compartir* sus datos.
- El 73,6% identifican la mejora de las posibilidades de la investigación médica como una razón para apoyar la transferencia de datos médicos

También es de interés observar los resultados del estudio realizado por *Salud Coop. (Ideas for Change y Mobile World Capital Barcelona Foundation)*[1092] donde detallan los riesgos y beneficios de proporcionar datos personales a diferentes destinatarios (sector privado, sector público, o cooperativa):

	Individual	*Privada*	*Pública*	*Cooperativa*
Escenario	María almacena sus datos de salud disco duro.	María almacena sus datos de salud en una plataforma propiedad de una empresa privada (por ejemplo, ***Apple Health*** u otro PHR app)	Los datos de María se almacenan en varias bases de datos propiedad de **instituciones públicas**. (p. ej.la Meva Salut). María tiene un nombre de usuario para acceder a sus datos	Los datos de María se almacenan en diferentes bases de datos. María tiene un nombre de usuario para acceder a sus datos, y los comparte con la cooperativa **bajo condiciones específicas que ella ha establecido.**
Beneficios	- *Autonomía*: los individuos no dependen de otros para decidir qué hacer con sus datos. - *Control:* los individuos tienen el máximo control sobre sus datos, por lo que hay un mínimo temor sobre el potencial mal uso de los mismos.	-*Incentivo directo a los individuos*: reciben servicios y productos a cambio que les permitan acceder y gestionar sus datos de forma sencilla. -*Capacidad tecnológica:* se percibe que las empresas tienen un alto nivel de capacidad tecnológica.	- *Gran volumen de datos.* - *Garante del uso de los datos*. Las instituciones públicas son percibidas como buenos garantes del uso de los datos, ya que sus **los objetivos son de interés público.**	- *Modelo integrador*: la cooperativa puede integrar datos de diferentes fuentes de información, tanto públicas como privadas (hospital, clínica privada, y prendas de vestir). Esto permitiría que los diferentes tipos de información fueran integrado y correlacionado, incluyendo hábitos, sensores e

[1092] Vid. https://static1.squarespace.com/static/57c55d71725e25ba4eb91756/t/58e533fb1b631bedcc67acad/1491416088875/Salus+coop.pdf

				historias clínicas. - *Decisión guiada*: las personas dispuestas a donar sus datos de salud pueden ser informados y asistido por la cooperativa. - *Independiente de los cambios políticos*.
Riesgos	*-Los datos no son muy valiosos* para la investigación, ya que el valor de los datos personales reside en su agregación. - *Pérdida de datos*: si se pierden datos, los individuos no pueden Reclamar a terceros porque los datos estaban en un almacén personal. - *Aislamiento*.	- *Finalidad última de los datos:* la gente tiene poco o nada de conocimiento de lo que las empresas hacen con sus datos. Los términos de uso que la gente firma de usar el producto son a menudo difíciles de entender. Un punto clave es que algunos usuarios pueden no estar al tanto del ***uso secundario*** de sus datos. - *Sin interoperabilidad*: en general, las empresas no tienen acceso a los historiales médicos de los centros de salud. - *Riesgo de pérdida de datos*.	- *Cambios políticos*. - *Poca capacidad de inversión*: (soluciones tecnológicas, o bien podría ser una falta de incentivo para acelerar la investigación en de la salud). - *Riesgo de pérdida de datos:* La lentitud podría afectar a la gestión general de la de intercambio de datos, - *No hay una decisión directa del ciudadano:* (sobre el uso secundario de los datos de salud.)	- *Falta de incentivos individuales*: puede haber una falta de interés si la gente no ve cómo se benefician. - *Falta de masa crítica:* motivar a un gran número de personas a participar. *-Complejidad del modelo de gobernanza*: especialmente con respecto a la creación de confianza y transparencia, y garantizar el interés público. *-Dificultad para acceder a los datos*.

Tabla 53. Cuadro comparativos de los beneficios y riesgos de otorgar datos personales según los encuestados.

3.2. El titular como *propietario* del dato personal.

El sector de la informática sanitaria, refiriéndose al ámbito de los datos masivos, lo tiene claro: *"la propiedad es de las personas* (…), aunque el valor[1093] de los mismos

[1093] Recientemente, senadores estadounidenses (demócratas y republicanos) presentarán una legislación para exigir a Fb, Google, Amazón y otras plataformas revelen el valor de los datos de los usuarios (datos de ubicación, estado de la relación, datos sobre las aplicaciones que utilizamos, nuestra edad, género y estilo de vida. El valor suele rontar los 5 dólares al mes, mientras en otras estimacines se calcula los 20 dólares. El proyecto de ley incluye medidas como: (i) Exigencia a las empresas que generen ingresos a partir de la recopilación de datos con más de 100 millones de usuarios mensuales, de revelar a los usuarios los tiepos de datos recopilados, cómo se utilizan y proporcionan una evaluación del valor de los mismos; (ii) revelación anual a la Comisión de Valores e Intercambio, del valor agregado de todos los datos, cómo los ingresos son generados por los datos del usuario y las medidas tomadas para proteger esos datos; (iii) Desarrollo de métodos para calcular el valor de los datos del usuario, teniendo en cuenta

puede ser regulado, puede ser utilizado con fines lícitos por parte de las organizaciones o entidades que los producen".

La conclusión no es que en cualquier caso se pueda utilizar, sino que hay que definir para qué se va a utilizar"[1094]. Desde el sector médico, se defiende en este sentido *"los datos no son solo del paciente, pues las historias clínicas tienen mucha información útil"*[1095].

Después de haber analizado la preocupación por la privacidad de las personas y llegados a este punto del trabajo, cabría preguntarnos; ¿el derecho de protección de datos podría convivir con el derecho de propiedad?; ¿son compatibles?; ¿en qué se diferencian?

Para poder contestar partimos de las ideas principales siguientes;

i. Todo ser humano tiene *ciertos* derechos que le otorgan privilegios o beneficios contemplados en leyes o que se organizan y desempeñan en los distintos espacios donde se desenvuelve éste.

ii. Los derechos en las personas no están sujetos a preferencias de nacionalidad, residencia, origen étnico, color, lengua, sexo u otra condición que discrimine a unas personas de otras.

iii. El derecho fundamental de protección de datos es un derecho humano (art.12. Declaración Universal de los Derechos Humanos de 1948).

---

los diferentes usos, sectores y modelos de negocios. Por su parte, las empresas argumentan que no es posible calcular el valor exacto de datos específicos. Vid. https://www.axios.com/mark-warner-josh-hawley-dashboard-tech-data-4ee575b4-1706-4d05-83ce-d62621e28ee1.html

[1094] XXIII Jornadas Nacionales de Informática Sanitaria en Andalucía 'Innovación y Salud', un evento organizado por la Sociedad Española de Informática de la Salud (SEIS). Ver artículo http://www.elmedicointeractivo.com/articulo/reportajes/big-data-sanitario-herramienta-aun-desconocida/20161025143034106859.html

[1095] Valdivieso, B. y Peiró, S. Presentación del informe *"Big data y Salud"* Planner Meida y Prodigioso Volcán, Roche Farma y Siemens. Recuperado de http://haycanal.com/noticias/8617/Big-Data--Los-datos-en-salud-pueden-salvar-vidas

iv. Se requerirá tener bien diferenciado los conceptos de "derechos reales" y "personalísimos".

Los derechos reales son el poder jurídico que una persona puede ejercer sobre algo de forma directa e inmediata para aprovecharla total o parcialmente. Respecto a los derechos personalísimos (o derechos de la personalidad), se puede decir que son inalienables, indisponibles, irrenunciables, indivisibles, universales e imprescriptibles.

El derecho fundamental de protección de datos no se puede entregar, transferir o vender. Los derechos humanos son derechos intrínsecos y evidentes por sí mismos, al margen de que estén envueltos y protegidos por regulación y codificación externa a través de diferentes leyes constitucionales en cada parte del mundo. Estos derechos existen por sí solos al margen de la diferente regulación. Tenemos que tener presente que el hecho de que "algo" sea similar a una propiedad, no significa que lo sea o deba ser bajo la ley (de turno) de propiedad. Al igual que las leyes constitucionales (y de desarrollo nacionales e internacionales) de derechos humanos regulan los derechos de personalidad, también pueden proteger "cosas" similares a la propiedad con características similares a la propiedad. Se podría dejar abierta la posibilidad de que "algunos" datos personales podrían existir en forma de propiedad.

Imaginemos por un momento que pudiéramos *cambiar "datos" por "medicamentos"* o *"datos" por "servicios de salud privados"* (tele consulta, etc.). Ceder información personal a cambio de una retribución, descuentos o similar cada vez es más posible, y más aún, con la expansión de la tecnología *blockchain* y DLT en la Industria de la Salud[1096].

O pensamos en la posibilidad de empoderar al individuo otorgándole herramientas para gestionar los datos y monetizar datos personales. Eso es posible con aplicaciones como *CitizenMe, People.op, Hat Community Foundation, CTRL.io ,Cozy.io, Digi.me o Meeco* (y más de cien) que compiten contra *Google, Fb, Amazon,*

[1096] La empresa española *PrivacyCloud* ha desarrollado *Werule,* una aplicación móvil que permite cambiar información personal por servicios[1096]. *Spotify*, por ejemplo, usa esa plataforma y permite que el usuario decida compartir información como la edad, el estado civil o sus gustos concretos, y a cambio proporciona al usuario puntos canjeables para los usuarios.

Equifax, Experial, etc. Así por ejemplo, la aplicación móvil *CitizenMe*[1097] posibilita que el mercado pague a los ciudadanos directamente por datos anonimizados y agregados referidos a la identidad, hogar, salud, economía, etc. que tiene clientes como la Universidad de Cambridge, de Bath o Manchester.

Pero más allá del intercambio de cesión de datos por servicios facilitado por tecnología o de la monetización directa por datos anonimizados agregados, hay quien piensa que podría existir una compensación ("*royalties*")[1098] dirigida a los individuos que hubieran contribuido a generar ingresos y a tomar decisiones en un sistema de IA. Por su parte, la abogada *Reinieris* (2018) señala que:

> "Todas las cosas digitales, ya sea dinero como moneda digital, credenciales como un pasaporte digital o obras de autor, son relativamente indistinguibles cuando se expresan como datos, cada una de las cuales consta de bits y bytes compuestos de dígitos binarios (es decir, 0s y 1s). Pero el dinero y el habla, cuando se expresan como datos, son cualitativamente diferentes de sus versiones no digitales. Esto tiene que ver con la naturaleza misma de los datos (…) Los datos transmiten liquidez y transferibilidad. Una vez digitalizados, los datos sobre nosotros (es decir, los datos personales) se convierten en "dinero" y adquieren una calidad transferible o transaccional"[1099].

Esta visión nos lleva a reflexionar éticamente acerca de la una posible suerte de "propiedad del dato" en la Era del petróleo de los datos y de la economía digital. Debido al gran valor comercial que pueden alcanzar resulta una cuestión bastante polémica para diversos actores o *stakeholders*[1100]. La concepción del dato como propiedad que puede

[1097] Vid. https://drive.google.com/drive/folders/1FJ1hnK8sO-7WD7VTVsZ81t4jHn8uYD6e Diap. 12

[1098] El científico de datos de la ONU, *Miguel Luengo* se cuestiona, por ejemplo, si deberían los médicos recibir compensación económica cada vez que la IA detecte un tumor basado en los diagnósticos que ellos hicieron en el pasado. Este autor propone "que aquellos *cuyas acciones valgan para entrenar modelos* sean compensados cada vez que se usen". Es decir, va más allá, no solo propone que se pague una contraprestación (entiendo, que al titular de los datos) sino cada vez que se contribuye y a quien contribuye a crear "máscaras para el *deep learning*". https://retina.elpais.com/retina/2019/01/04/tendencias/1546604928_551805.amp.html.

[1099] https://medium.com/@hackylawyER/money-talks-how-digital-money-speech-challenge-existing-legal-frameworks-dd845a7ceaf7

[1100] Ahora bien, ¿las nuevas empresas y aplicaciones, como las que hemos mencionado, que se están preocupando (y ocupando) sobre esta cuestión podrían solucionar esta cuestión? Parece que no será suficiente. La implicación de todos los *stakeholders* es muy necesaria (gobiernos, tecnológicas, científicos de datos, desarrolladores, industria, ciudadanos, consumidores y usuarios, etc…). El pacto social podría

ser vendido, comprado o alquilado podría derivar a lo que denomina esta autora como "modelo de tecnología publicitaria de Internet" (Reineieris, 2018)[1101]. Para ella, puede resultar algo peligroso ya que esta tendencia puede convertirse en un "modelo de tecnología publicitaria rota de Internet" extendido a todas las facetas de nuestra identidad digital.

Por su parte, el investigador *Christopher Olk*[1102], aboga más bien por una visión de *"los datos como intelecto general"* de una sociedad, tomando la vertiente del pensamiento del postoperacionismo o del marxismo y, esto implicaría que los datos más que ser un producto de cada individuo pertenecerían a la sociedad entera.

Para *Shanon Vallor*[1103], "parte de la propiedad de los datos tiene que ver con el control sobre nuestra persona, el control sobre la historia que se cuenta sobre nosotros y el control sobre lo que podemos saber sobre nosotros. El significado de los datos es algo de lo que la persona que genera los datos nunca puede separarse por completo[1104].

Pero atención, al margen de todo ello, no olvidemos la importancia de la ética y la moralidad individual; "los consumidores deberán comprender los beneficios y la responsabilidad que conlleva la propiedad y el control de sus datos de soberanía para la adopción exitosa de nuevos servicios increíbles" (Maaghul)[1105].

---

llegar con propuestas y diálogo abordando los modelos de negocios de la Industria y regulación (o autorregulación).

[1101] https://medium.com/@hackylawyER/do-we-really-want-to-sell-ourselves-the-risks-of-a-property-law-paradigm-for-data-ownership-b217e42edffa

[1102] https://www.youtube.com/watch?v=d36eDT4lPWc

[1103] Vid. https://www.scu.edu/ethics/internet-ethics-blog/on-data-ethics-an-interview-with-shannon-vallor/

[1104] En la medida en que los datos representan aspectos de nosotros mismos de los que no podemos separarnos, y en la medida en que los datos pueden utilizarse para beneficiarnos, dañarnos, exponernos o protegernos, debemos tener una capacidad. Para entender lo que está en juego transfiriendo esos datos. Tiene que haber condiciones reales, condiciones significativas, puestas en su uso. Es difícil tener esas condiciones si existe la presunción de que no somos dueños de nuestros datos o si existe la presunción de que en el momento en que generamos los datos en un espacio visible, podemos separarlos de nosotros como propiedad de otra persona. y en la medida en que los datos puedan utilizarse para beneficiarnos, perjudicarnos, exponernos o protegernos, debemos tener la capacidad de comprender la importancia de transferir esos datos. Tiene que haber condiciones reales, condiciones significativas, puestas en su uso. Es difícil tener esas condiciones si existe la presunción de que no somos dueños de nuestros datos o si existe la presunción de que en el momento en que generamos los datos en un espacio visible, podemos separarlos de nosotros como propiedad de otra persona. y en la medida en que los datos puedan utilizarse para beneficiarnos, perjudicarnos, exponernos o protegernos, debemos tener la capacidad de comprender la importancia de transferir esos datos. Tiene que haber condiciones reales, condiciones significativas, puestas en su uso. Es difícil tener esas condiciones si existe la presunción de que no somos dueños de nuestros datos o si existe la presunción de que en el momento en que generamos los datos en un espacio visible, podemos separarlos de nosotros como propiedad de otra persona."

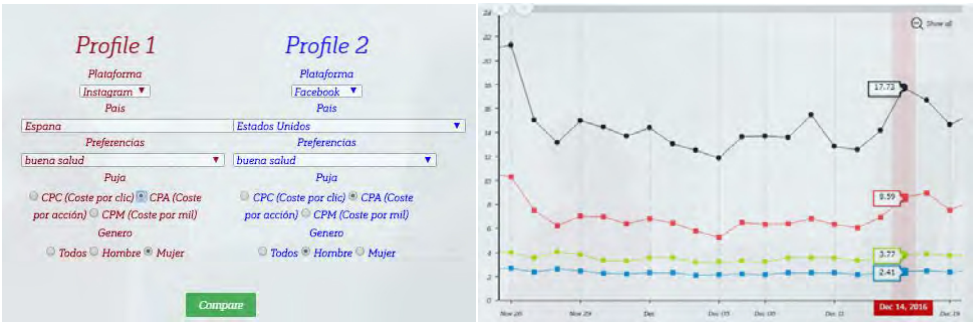
[1105] Vid. https://www.pointnurse.com/blog/do-you-have-a-healthcare-blockchain-strategy/

Y, *¿cuanto "valen" los datos de salud?*

La Comisión Europea[1106] estimó el mercado de la información personal para el 2020 en 736.000 millones de euros. *Facebook*, por su parte, valoraba cada perfil de ciudadano europeo en 8,76 dólares en último trimestre de 2017, unos dos dólares más que la media mundial, pero cuatro veces menos que lo que ingresaba por un usuario de EEUU o Canadá, a los que tasaba en 26,86 dólares[1107].

Para el investigador Cuevas[1108], "se parece una bolsa de valores en la que anunciarse en los perfiles de los usuarios se rige por la oferta y la demanda". También ha concluido que "no todas las audiencias valen lo mismo: los hombres suizos interesados en banca online se cotizan al doble que los españoles, por ejemplo. Los perfiles no se ofertan individualmente, sino en grandes paquetes de usuarios que comparten intereses". La *Facebook Data Valuation Tool* (FDVT) es una app que se puede descargar para averiguar y medir cuánto valen los datos que está generando el usuario.

A continuación, señalamos un ejemplo[1109]:



[1106] Vid. https://ec.europa.eu/digital-single-market/en/news/final-results-european-data-market-study-measuring-size-and-trends-eu-data-economy

[1107] Vid. https://s21.q4cdn.com/399680738/files/doc_financials/2017/Q4/Q4-2017-Earnings-Presentation.pdf

[1108] Vid. https://www.eldiario.es/tecnologia/cotizan-mercado-Facebook-precio-fluctua_0_757675161.html#click=https://t.co/uwAnl74Len

[1109] Vid. http://testdeprivacidad.org/?page=iframe. La línea roja (mínimo) y negra (máximo) representa al valor de los datos de "buena salud" de la plataforma Instagram donde se hace perfilado de mujer española. La línea verde (máximo) y azul (mínimo) representa el valor de los datos de "buena de salud" de la plataforma Facebook donde se hace perfilado de hombre estadounidense. Como se puede el valor de los datos de salud de las mujeres españolas en Instagram alcanza su máximo valor el 14 de diciembre de 2016 (17,73 €). Quizás, tiene su explicación por la cercanía de las fiestas y cenas de navidad. Por el contrario el valor de los datos de salud de los hombres estadounidense es bajo (2, 41 €).

Imagen 84. Gráfico de valoración de los datos de salud en Facebok e Instragram por género. Fuente: Testdeprivacidad

En el 2015, los *datos genéticos* de *23andMe* valían 2.500 veces más por usuario que los de Facebook (Ver imagen superior) [1110]. *Genentech* pagaría hasta 60 millones de dólares (unos 48 millones de euros) por acceder a los 3.000 pacientes de Parkinson con base de datos de *23andMe*[1111]. Puede resultar escalofriante que 23andMe se aliara con una farmacéutica teniendo todo este poder masivo de datos genéticos, teniendo posible la mayor base de datos abierta a los estudios médicos, donde de sus 820.000 clientes, 600.000 han aceptado donar sus datos de ADN para objetivos de investigación. Esta empresa resalta la implicación de los consumidores en participar en las investigaciones. El impacto internacional puede ser bastante grande y el debate, también, al margen de que esté permitido la venta de los datos genética o no en las legislaciones nacionales[1112].

Hay quien habla[1113] de un concepto denominado como "retorno de datos" (ROD) que es igual a "utilidad que ganan los consumidores" entre "los datos que suministran (ROD = U/D). Por ejemplo, piénsese en el provecho que puede extraer un usuario de las redes sociales; ¿acaso los beneficios de los servicios son proporcionales? En este sentido, se sugiere incluso las preocupaciones de privacidad no deben ser vistas en forma aislada, sino como parte de ROD.

3.3. Mercado negro de datos de salud.

Por otro lado, no podemos desconocer la situación peligrosa del mercado negro o de la *deep web,* donde los datos médicos completos de un paciente son más valiosos que las tarjetas de crédito[1114], y según la FBI **se venden entre 20 y 70 dólares,** mientras que una tarjeta puede costar tan solo 5 dólares[1115]. El motivo puede ser el hecho de que hospitales y aseguradoras no tengan un protocolo claro para ayudar a los pacientes, además de que la inversión en tecnología es mayor en el sector bancario que en el sanitario. El tema no es nada baladí. Resulta preocupante saber que los

[1110] Vid. https://www.technologyreview.es/s/7332/los-datos-geneticos-de-23andme-valen-2500-veces-mas-por-usuario-que-los-de-facebook

[1111] Vid. http://www.forbes.com/sites/matthewherper/2015/01/06/surprise-with-60-million-genentech-deal-23andme-has-a-business-plan/

[1112] Vid. http://sitn.hms.harvard.edu/flash/2018/understanding-ownership-privacy-genetic-data/

[1113] https://www.schneier.com/blog/archives/2019/05/the_concept_of_.html

[1114] Vid. https://www.eldiario.es/hojaderouter/seguridad/hospitales-sanidad-seguridad_informatica-ciberataques-datos-privacidad_0_427657312.html

[1115] Vid. https://www.cbsnews.com/news/do-hackers-have-your-health-records/

ciberdelincuentes tendrían la posibilidad acceder a información tan sensible como alergias o grupo sanguíneo o el estado general de salud[1116], para obtener beneficio económico con la venta o con el secuestro de datos.

Un grupo de hackers chantajearon al laboratorio francés Labio para que entregaran un rescate económico para evitar la publicación de los registros de salud de los pacientes en el mercado negro, pero finalmente no entregaron dicho rescate y se publicó la información médica[1117].

Lo más llamativo para *Oren Koriat*, investigador de seguridad en *Cynerio*, es la tendencia de la venta de datos de salud de personas fallecidas[1118], motivada por la simple razón de que las personas fallecidas no podrían presentar reclamaciones judiciales por robo de identidad[1119], pudiéndose pasar la situación desapercibida durante mucho tiempo. Tal y como declara él, "cuando se trata de registros médicos, a menudo se utilizan en combinación con otra información personal para realizar transacciones fraudulentas aún más sofisticadas". Esto es peligroso y requerirá de una fuerte regulación. Según una consultora, los mayores problemas[1120] estaban en; (i) Hackear datos de proveedores para robar documentos administrativos, como licencias médicas, para falsificar la identidad de un médico. Estos datos se venden en la web oscura por alrededor de $ 500; (ii) Hackear la información de inicio de sesión de un proveedor de seguros y luego venderla a un comprador, quien luego puede restablecer las credenciales de la base de datos y tomar la identidad de la víctima para reclamar el seguro; (iii) Falsificar tarjetas de seguro médico, recetas y etiquetas de medicamentos con la intención de llevar medicamentos a través del aeropuerto; (iv) Uso de información médica personal pirateada contra personas que tienen problemas de salud por extorsión y otros delitos.

3.4. Datos personales para el bien común.

Ya lo dijo el experto de privacidad *Sam Smith* en relación con el *caso Deep Mind Health /NHS*: "Los intereses vitales de un paciente hipotético no son intereses

---

[1116] Se han dado situaciones donde se roba la identidad de personas que tienen buena salud y son secuestradas y víctimas para el tráfico de órganos

[1117] Vid. https://www.mcafee.com/es/resources/reports/rp-hidden-data-economy.pdf (El comercio clandestino de datos de salud).

[1118] Vid. https://threatpost.com/deceased-patient-data-being-sold-on-dark-web/133871/

[1119] Los estafadores intentan robar las identidades de 2,5 millones de estadounidenses fallecidos cada año en un intento de abrir cuentas de tarjetas de crédito, solicitar préstamos, cometer fraudes fiscales y obtener costosos teléfonos móviles a través de contratos de operadores. Para más info: https://www.aarp.org/money/scams-fraud/info-03-2013/protecting-the-dead-from-identity-theft.html

[1120] Vid. https://thenextweb.com/security/2019/06/11/hackers-are-stealing-personal-medical-data-to-impersonate-your-doctor/amp/

vitales de un sujeto de datos real. El único *interés vital* protegido aquí es el de Google, y su deseo de acaparar los registros médicos que se le informaron fue recopilado ilegalmente[1121].

¿Y si vemos a los datos personales como *empoderamiento colectivo*[11221123]?

La investigadora *Prince Ball*[1124], en el *MyData2018*, señaló que "nuestros datos personales son contextuales y se entremezclan con los datos de otros; el poder surge de la agregación". Declaró en palabras de *Bárbara Evans*, que "cuando nos centramos en el poder individual ("autonomía atomística") no nos empoderamos plenamente a nosotros mismos si los problemas a los que nos enfrentamos requieren una acción colectiva. Ambas consideras que podríamos aprender de la bioética, un campo con enfoque atomístico que no alcanza a dar un verdadero empoderamiento.

4. LA ÉTICA DE LOS DATOS Y LAS ORGANIZACIONES.

4.1. La ética de los datos y RSE

4.1.1. ***¿Qué es la ética de las organizaciones o empresarial?***

La ética tiene una gran importancia en la sociedad, dado que los individuos la aplican en su día a día con el fin de decidir las mejores soluciones a los problemas con los que se van enfrentando. Esta disciplina busca expresar de una forma razonada qué actitudes y acciones deben llevarse a cabo con el fin de lograr el perfeccionamiento de la sociedad y, por tanto, de cada uno de sus individuos. Según el manual de

[1121] Vid. https://www.theregister.co.uk/2018/06/13/royal_free_deepmind_deal_audit/

[1122] Pero, ¿qué es la acción colectiva? Podría considerarse como un esfuerzo colectivo que ayuda a aumentar la autonomía donde la gente se compromete y está más informada. La investigadora Price, resalta dos ejemplos en el ámbito de la tecnología que podrían ser llamados como ejemplos de "producción social" (*Yochai Benkler*) que son *Linux* (software de forma colectiva que empezó como modelo y acabó como infraestructura) y *Wikipedia* (quinto sitio más popular de la web).

[1123] Vid. https://www.gov.uk/government/news/ndg-poll-findings-public-attitudes-to-organisations-innovating-with-nhs-data

[1124] En este sentido *Open Humans* (Vid. https://www.openhumans.org/) donde trabajó la investigadora, ha ayudado a miles de personas a aportar datos para hacer posible una investigación comunitaria. Pero, ¿cómo hacerlo posible? Señala que los modelos de producción *peer two peer* son poderosos y que una vez que algo se convierte en infraestructura casi imposible de cambiar. *OpenAPS* (vid. https://openaps.org/) es una plataforma abierta y transparente que permite formada por una comunidad que ha creado un diseño que permite que que por la noche se estime la glucosa en sangre para ajustar automáticamente los niveles de insulina.

Deres[1125],asociación de empresarios uruguaya, "las normas éticas son imperativos que facilitan que los principios éticos puedan llevarse a la práctica. Entre ellos, contamos con el deber de la veracidad, el respeto a la intimidad y privacidad y el cumplimiento de los acuerdos, la lealtad".

Por tanto, podríamos considerar a los derechos fundamentales de intimidad y privacidad como principios éticos. El término de "ética empresarial" nació en los EEUU aunque fue en Europa donde se creó la asociación *European Business Ethics Network* (EBEN), cuyo objetivo era principalmente desarrollar la ética empresarial en Europa. En la década de los 90, los escándalos de Enron provocaron de nuevo su interés. Ahora, las empresas entienden la importancia de que existan departamentos que administren la ética no sólo su adecuación con la misión y valores que quiere reflejar la empresa, sino también por los aspectos que las organizaciones éticas traen de la mano.

En el siglo XXI la sociedad exige ser informada de las actuaciones de las empresas, exige responsabilidades. Esta visión parece hacer referencia a la comúnmente conocida como *"responsabilidad social empresarial*", un término que aunque relacionado, no significa lo mismo que *"ética empresarial"*. En muchas ocasiones se confunden.

Ética Empresarial	***RSE***
Ref. a ***comportamientos o actuaciones*** considerados como ***correctos*** dentro de la empresa	Ref. al ***conjunto de actividades*** que esta realiza para controlar su impacto.
Condicionados por *stakeholders*	*Puede haber código ético o no*

Tabla 37. Diferencias entre ética empresarial y RSE

4.1.2. ***¿Qué es la ética de los datos?***

Para responder, en primer lugar partamos de la definición citada de los autores Floridi y Taddeo (2016); "una nueva rama de la ética que estudia y evalúa los problemas morales relacionados con los datos (incluida la generación y el registro), curación, tratamiento, difusión, puesta en común), algoritmos (incluida la inteligencia artificial, de los agentes artificiales, el aprendizaje automático y los robots) y prácticas correspondientes (incluidas las prácticas responsables de innovación, programación,

[1125] DERES."Manual para elaborar CÓDIGOS DE ÉTICA EMPRESARIAL", Uruguay. Recuperado de http://deres.org.uy/wp-content/uploads/Manual-de-Etica-DERES.pdf

hacking y profesionales de los códigos), con el fin de formular y apoyar moralmente buenas soluciones (por ejemplo, conductas correctas o valores correctos)"[1126].

De todo ello, se podrían extraer las siguientes conclusiones:

i. Es una *nueva rama* de la ética que profundiza sobre los *problemas morales* relacionados con los datos.
ii. Los problemas morales pueden surgir a raíz de :
    a. los *tratamientos de datos*: registro, modificación, difusión, comunicación, cesión. Desde mi opinión, se podría extender a las operaciones que señala el legislador en el art. 4.2. RGPD como la recogida, organización, estructuración, conservación, extracción, consulta, cotejo o interconexión, limitación, supresión o destrucción.
    b. los *algoritmos y sus prácticas* de los algoritmos: programación, hacking y otras.
iii. El objetivo es formular y apoyar moralmente *soluciones* como
    a. *conductas* correctas;
    b. *valores* correctos.

Pero ¿cómo definir lo que es correcto de lo que no? ¿Qué conductas de las organizaciones serán correctas? ¿y qué valores de las organización serán los correctos?

Estas cuestiones y otras intentaremos resolver a lo largo de este capítulo.

A la hora de potenciar la ética, son diversas las herramientas que pueden ser empleadas para imponer dentro de la empresa una serie de valores y preceptos éticos fundamentales. Entre estas herramientas, podemos contar con los códigos de ética empresarial, las estructuras éticas y las denuncias (Daft, 2003).

4.1.3. ***¿Qué es la RSE y por qué es importante en nuestro contexto?***

Como decíamos RSE no significa lo mismo que "ética empresarial". La responsabilidad social empresarial se refiere al conjunto de actividades que ésta realiza para controlar su impacto por medio de códigos éticos o no.

[1126] *Supra Cit.*

La responsabilidad social empresarial, desde el enfoque de la protección de datos y privacidad, se podría definir como *la contribución activa y voluntaria al mejoramiento social que tiene por objetivo mejorar la situación competitiva y valorativa de la empresa teniendo en cuenta el respeto del derecho fundamental de la protección de datos de las personas*.

Hemos de tener en cuenta que la *RSE va más allá del mero cumplimiento de la normativa*, por ejemplo, la RGPD, y tendrá un papel muy importante que se traducirá en la búsqueda creativa de *técnicas y herramientas* que posibiliten y den solución de alguna manera a las incompatibilidades de las tecnologías con los derechos y libertades de las personas[1127].

4.2. La ética impuesta

Está compuesta por herramientas que pueden ser utilizadas para "imponer" dentro de la empresa *valores y preceptos éticos*, como los códigos de ética empresarial y las denuncias internas.

4.2.1. ***Los códigos de ética de conducta o best practices.***

Son un conjunto de directrices que establecen las conductas correctas aceptables para los miembros que componen la empresa. Aplicar el código significará no solo respeta la legalidad, sino que irá más allá buscando la excelencia.

Será efectivo cuando sea *conocido y comprendido* por los empleados, para ello deben diseñarse planes de divulgación adaptados a la *formación* e instrucción profesional[1128].

[1127] La concienciación de esta ética no solo repercute en beneficio de los clientes sino de la propia sociedad. Pensemos, por ejemplo, en el tratamiento de datos personales de historiales clínicos electrónicos por parte de empresas farmacéuticas y consorcios con las empresas tecnológicas en el marco de investigaciones científicas donde el impacto puede ser mayor habida cuenta el desequilibrio de poder de los diferentes *stakeholders*. Disponible en línea: https://elpais.com/tecnologia/2016/06/22/actualidad/1466608415_759681.html . Según los desarrolladores se hace hincapié en la psicooncología y hábitos de la paciente

[1128] Por ejemplo, planes de capacitación para los empleados (de una aseguradora de salud, los desarrolladores de una aplicación de inteligencia artificial, los investigadores que tratan datos de salud, etc). La empresa debe explicar por qué era necesaria su creación, así como de qué forma debería de utilizarse, su misión y las consecuencias de su transgresión o incumplimiento. La difusión o publicación de los códigos será interesante y necesaria para hacerlos llegar a todos los grupos de interés implicados como clientes, proveedores, subproveedores, y usuarios y titulares de datos personales. Además, con el fin de conseguir su cumplimiento podrían utilizarse estímulos y sanciones o correcciones. El manual

Según la autora FERNANDEZ (2010) existirían dos tipos de códigos de conducta; los basados en principios corporativos (más generales y con objeto de crear cultura corporativa) y los basados en políticas (más específicos) donde podrían incluirse la confidencialidad, etc.[1129]

En definitiva, los códigos de conducta o best practices articularán el *desarrollo de la conducta organizada para la toma de decisiones* teniendo en cuenta ciertos valores, como el del respeto de los derechos humanos y libertades de las personas, y en particular, la propia *privacidad y la protección de datos de las personas*.

4.2.2. ***Canal de denuncias internas.***

Las denuncias por parte de los empleados ante incumplimiento de los principios o políticas éticas en materia de privacidad y protección de datos, confidencialidad o intimidad pueden llevarse a cabo de forma externa o interna. Las denuncias externas son aquellas que se realizan fuera de la empresa, informando a instituciones como pueden ser las agencias de gobierno (en nuestro caso, la AEPD). Las denuncias internas se dan cuando el individuo decide que debe ser un alto mando de la empresa el informado sobre las faltas que están produciendo (por ejemplo, al DPO). Con la nueva normativa se podrán hacer denuncias anónimas y se deberán informar a los empleados y a terceros de la existencia del canal de denuncias, además de adoptar las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos del denunciante. Los datos sólo se podrán conservarse el tiempo imprescindible para la averiguación de los hechos denunciados[1130].

4.3. Comités de ética en empresas.

DERES anima a crear herramientas como una sección de preguntas frecuentes, buzón, correo electrónico. Entre las ventajas más interesantes que proporcionan podrían estar la de mejorar la imagen de la empresa ante la sociedad y permiten ganar respeto y lealtad por parte de los clientes, proveedores y comunidades; sirve como guía de actuación ante posibles conflictos; se genera confianza entre los inversores; se facilita la captación de buenos clientes, proveedores, empleados, distribuidores que buscan empresas en las que confiar que compartan su ética.

[1129] Fernández, R. (2011). Códigos éticos o de conducta. Su concepto. Su necesidad. *Diario Responsable.* Recuperado desde http://diarioresponsable.com/opinion/14404-codigos-eticos-o-de-conducta-su-conceptosu-necesidad

[1130] Con la nueva normativa se podrán hacer denuncias anónimas y se deberán informar a los empleados y a terceros de la existencia del canal de denuncias, además de adoptar las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos del denunciante. Los datos sólo se podrán conservarse el tiempo imprescindible para la averiguación de los hechos denunciados.

Después de que los altos mandos hayan decidido que la creación del código ético es necesaria, se debería proceder a la creación de un comité de ético formado integrantes de primer nivel. Debe estar formado por consejeros independientes, piénsese, en el DPO, CCO, o externos como consultores especialistas en protección de datos, abogados, etc. Ahora bien, debido al contexto de estas organizaciones y entidades en el ámbito de la tecnología de la información y las tecnologías emergentes como IA, big data, blockchain, etc., deberíamos hablar de un comité "multidisciplinar" incluyendo a los desarrolladores internos (o externos) e ingenieros informáticos y de telecomunicaciones. La participación de todos ellos será fundamental. En su conjunto, el comité, se encargarán de elaborar el código pero se dejará la participación abierta a los empleados a los que se consulte. Y como hemos dicho anteriormente, se necesitará que la empresa defina quiénes son las personas que cumplirán con el código ético (empleados, proveedores, empresas colaboradoras, subproveedores, etc.).

En este sentido, el profesor Puyol señaló que las empresas además de implementar los comités internos de ética, en el caso de proyectos de IA, se podrían **desarrollar *colaboraciones sectoriales* para formular y compartir mejores prácticas**, concienciando al público donde se abriera discusión sobre los beneficios y los retos derivados de la inteligencia Artificial. Vid. https://confilegal.com/20181223-la-etica-y-la-responsabilidad-derivada-del-uso-de-los-algoritmos/

4.4. La necesaria autoevaluación.

La autoevaluación será una herramienta voluntaria e imprescindible para analizar y valorar las limitaciones de la organización en cuestiones de ética de los datos.

Retomemos los principios de las autoras Tranberg y Hasselbach (2018) para diseñar posibles ítems a incluir en un cuestionario o *checklist*, señalados acertadamente por estas autoras, que permitan a las organizaciones realizar una *autoevaluación*:

i. *"El ser humano como centro de todo.*

- ¿se utilizan los principios de privacidad por diseño?
- ¿se describen los fines del tratamiento de datos de manera clara y directa?
- ¿se aseguran de que los usuarios tengan *propiedad* (de los datos) en lugar de los intereses comerciales o institucionales? (Desde mi opinión, y siguiendo la premisa inicial de incluir como principios y valores a los propios derechos y libertades de las

personas, y en particular, al derecho de privacidad y protección de datos, incluiría el derecho de protección de datos de las personas fallecidas y derecho al testamento digital -Art. 3 y 96 LOPDGDD- en tanto que puede ser factible que se traten en el contexto de estudio de este trabajo).

ii. El control de los datos individuales.

- ¿se aseguran de que en la medida de lo posible el tratamiento de datos se realiza directamente en los dispositivos?
- ¿cuándo se realiza el tratamiento a través de una solución cloud, los datos personales recopilados son identificables (o anonimizables)?
- ¿se realiza *profiling*?¿se permite al usuario determinar los valores y reglas del mismo?
- ¿para el uso de predicciones de comportamiento se usan datos individuales o patrones?

(De igual modo en el punto ii. incluiría cuestiones que pueden afectar a los empleados y a sus derechos digitales en virtud de la LOPDGDD, como por ejemplo, el derecho a la intimidad en el contexto laboral con dispositivos, etc.)

iii. La transparencia.

- ¿en qué país se almacenan los datos personales? ¿dónde está el proveedor? ¿hay transferencias internacionales?
- ¿hay aprendizaje automático o *deep learning*? ¿se pueden explicar los criterios y parámetros de los algoritmos?
- ¿utiliza datos personales para influir en el comportamiento del usuario?
- ¿opera con software de código abierto, para que otros puedan usarlo y posiblemente desarrollarlo más? (Se podrían añadir más, como, por ejemplo, ¿cuenta con certificaciones, sellos de calidad o su empresa se ha adherido a un código de conductas de su autoridad de control nacional o sectorial?)

iv. La responsabilidad.

- ¿cuándo se anonimizan los datos personales?¿se utiliza encriptación de datos de extremo a extremo?
- ¿minimiza el uso de metadatos y explica cómo se hace?
- ¿usas el *conocimiento cero*[1131] como principio de diseño?
- ¿utiliza cookies de terceros?
- ¿utiliza *Google Analytics* o herramientas de seguimiento similares?
- ¿se venden datos a terceros?
- ¿se venden datos como datos personales identificables? ¿se venden datos como patrones en un nivel agregado?

[1131] Según Wikipedia, "en criptografía, un protocolo de *conocimiento cero* o prueba de conocimiento nulo, también conocidas por las siglas ZKP (del inglés *Zero Knowledge Proof*), es un protocolo criptográfico que establece un método para que una de las partes pruebe a otra que una declaración (generalmente matemática) es cierta, sin revelar nada más que la veracidad de la declaración.

- si venden datos, ¿se asegura de que se trate de información totalmente anónima que solo describa patrones y no individuos?
- ¿enriquece los datos con datos externos, como con datos de redes sociales o datos comprados? ¿Este enriquecimiento ocurre en respuesta a sus usuarios o en cooperación con ellos?
- ¿cuentan con un profesional o un departamento responsable de la gestión ética de los datos? ¿cómo se integra el trabajo con ética de datos en la organización?
- ¿necesitan y controla la ética de los datos de sus subcontratistas y socios?
- ¿cómo se asegura de que se respeten sus directrices de ética de datos? (Desde mi punto de vista, añadiría expresamente si la organización cuenta con código de conductas para trabajadores (régimen sancionador) o proveedores (con penalización económica)
- ¿el proceso de datos puede ser auditado por un tercero independiente?

v. La igualdad.

- ¿participa en un diálogo con sus usuarios en una plataforma pública?¿tienes pautas para usar la plataforma? ¿modera la plataforma para eliminar datos personales confidenciales?
- si sus servicios se ofrecen a menores, ¿garantiza el consentimiento de los padres?
- ¿se usan los datos para desarrollar o entrenar un algoritmo?
- ¿se asegura de que el uso de los datos no lleve a la discriminación? ¿se asegura que el uso de datos no expone las vulnerabilidades de las personas? (Añadiría que medidas concretas se establecen para asegurar que no se produce discriminación algorítmica)
- ¿se asegura de que el uso de la inteligencia artificial / el aprendizaje automático beneficie a la persona y no cause daños físicos, psicológicos, sociales o financieros?"[1132].

[1132] Una vez analizados estos ítems, sería interesante tener en cuenta algunas *herramientas* que las autoras señalan acertadamente en la página web del *thing to tank "Dataethics"* dirigidas a las organizaciones que se han autoevaluado; (i) *"Sobre el uso de motores de búsqueda y alternativas.* Las empresas podrían recomendar el uso de estos motores de búsqueda diferentes a Google, como la británica *Mojeek*, la alemana *Startpage,* la francesa *Qwant,* la suiza *Hulbee* que no rastrean a los usuarios ni almacenan todas las búsquedas o el uso de *Cludo* basado en IA para marketing, sitios web y contenido. (ii) *Sobre el uso de herramientas analíticas para medir el tráfico y obtener datos sobre visitantes y alternativas.* Existen herramientas como *Piwik* de código abierto que proclama la propiedad del 100% de los datos, o la danesa *Netminers* o el alemán *Webtrek* donde no se paga con datos sino con dinero. Y sobre plataformas que rastrean a los visitantes (como es *Google Analytics)* se puede utilizar *Typeform. (iii) Sobre alternativas a los complementos sociales.* Para evitar el seguimiento y control de los clientes con los botones Facebook, Google+, y Twitter, de manera que estos pueden realizar seguimientos y crear historiales de navegación incluso aunque no accione dichos botones. Por ello, las autoras aconsejan soluciones alternativas como *Social Share Privacy*. Ver en : http://panzi.github.io/SocialSharePrivacy/. (iv) Por defecto, solo está incrustada una imagen de maqueta gris de un botón similar. Solo si un usuario hace clic en este botón, se carga el botón de me gusta real y se envía información a la red social. Con un segundo clic, al usuario le puede gustar la página web (o tuitearla, etc.). (v) *Acerca de cookies de terceros.* Las autoras señalan claramente que, "hay muchas razones para considerar deshacerse de todos los rastreadores de

En definitiva, todo ello se resume a que una organización empresarial *será ética y responsable* desde el punto de vista de la privacidad, cuando actúa desde un punto de vista preventivo y no reactivo, usando herramientas de *privacy by design*, otorgando información clara al titular de los datos, adhiriéndose a *best practices* o códigos de conducta, creando medidas para evitar la discriminación algorítmica, etc. y se aplican los principios y valores de la nueva normativa europea y española de protección de datos.

4.5. Certificaciones y sellos de calidad de ética de datos.

No resulta fácil para los stakeholders, identificar a organizaciones que traten datos y que lo haga de una forma ética y responsable. Por ejemplo, en Australia ya existe una marca o sello denominado "*Fair Data"* [1133], que se puede otorgar al superar una auditoría independiente y se hayan comprometido con ciertos principios[1134]:

i. "El consentimiento (o legitimación del tratamiento). Nos aseguraremos de que todos los datos personales se recopilen con el consentimiento de los participantes / clientes. (Ahora bien, desde mi opinión, en el código ético se debería tener en cuenta la normativa europea y especificar que el consentimiento no es la única base legitimadora del tratamiento de datos)

ii. La utilización (o finalidad del tratamiento). No utilizaremos los datos personales para ningún otro propósito que no sea para el que se otorgó el consentimiento, respetando los deseos de los participantes / clientes sobre el uso de sus datos.

iii. El acceso. Nos aseguraremos de que los clientes tengan acceso a sus datos personales y les diremos cómo los utilizamos. (Además del derecho de acceso habría que asegurarse que la organización está en disposición de ejercitar todos los demás del RGPD y LOPDGDD).

---

terceros. Especialmente si trata con datos, muchos consideran sensibles como la salud, las finanzas y la política. La Comisión de la UE no permite cookies de terceros en su sitio web[1132]". (vi) *Acerca de soluciones seguras en Cloud Computing.* Las autoras señalan los sistemas alemanes *T-Systems* y Tresorit , la danesa Rushfiles o la francesa *Cozy* o incluso optar por construir la propia nube de empresa.
Acerca de los grupos de Facebook, Skype. Las autoras señalan que "muchas organizaciones sin fines de lucro, autoridades públicas y pequeñas empresas optan por utilizar grupos en Facebook en lugar de usar sus propios sitios web o una alternativa segura, incluso con datos sensibles como datos de salud. Una buena alternativa es *Groupcare,* que tiene su sede en Dinamarca". Y respecto a alternativas de skype para proteger la privacidad se puede optar como la suiza Wire". Para más info: https://dataethics.eu/en/tools/

[1133] Vid. https://probonoaustralia.com.au/news/2018/11/ethical-trust-mark-promotes-fair-data-use-australian-businesses/

[1134] Vid. http://fairdata.com.au/the-10-fair-data-principles-consumer/

iv. La seguridad. Protegeremos los datos personales y los mantendremos seguros y confidenciales. (Sería conveniente distinguir claramente entre "confidencialidad", "seguridad" y "privacidad").

v. El respeto. Nos aseguraremos de que el personal entienda que los datos personales son solo eso, personales, y garantizaremos que se traten con respeto.

vi. La protección. Nos aseguraremos de que las personas vulnerables y menores de edad estén debidamente protegidas por los procesos que utilizamos para la recopilación de datos.

vii. La cadena de suministro. Gestionaremos nuestra cadena de suministro de datos con los mismos estándares éticos que esperamos de otros proveedores.

viii. La obtención (o recogida). Aseguraremos que las mejores prácticas éticas en datos personales sean parte integral de nuestro proceso de adquisición.

ix. La formación. Nos aseguraremos de que todo el personal que tiene acceso a los datos personales esté debidamente capacitado para su uso.

x. La reputación. No utilizaremos datos personales si existe incertidumbre sobre si se han aplicado los Principios de Datos Justos.

Aunque puede resultar demasiado escueto este elenco de principios, no se puede desmerecer este tipo de iniciativas, que abrirán el camino a otras nuevas, actualizadas y adaptadas a sectores y tecnologías.

4.6. Ética desde el diseño ("Ethic by design")

El que fue filósofo y desarrollador de Google, *Tristan Harris*, señaló que **"**Apple y Google, como todas las empresas, responden a lo que demandan los consumidores. Cuando la ***privacidad*** **se** volvió importante para ti, ellos respondieron. Desarrollaron nuevas características de privacidad y seguridad, y provocaron una nueva conversación y debate público. Ahora es la preocupación más popular sobre la tecnología discutida en los medios" [1135].

Los diseñadores tienen una gran responsabilidad ética con la sociedad y los derechos y libertades de las personas. "La formación filosófica ofrece unas capacidades

[1135] Vid. http://www.tristanharris.com/the-need-for-a-new-design-ethics/

muy valiosas para las empresas tecnológicas y, en general, para el desarrollo que viven actualmente la ciencia y la tecnología" (Mendoza, 2017).

Con las tecnologías emergentes, los desarrolladores se han visto enfrentados a la duda de cómo encontrar equilibrio entre desarrollar tecnología "éticamente y responsablemente" para la sociedad y los negocios, *per se*. Esto hace que inevitablemente la responsabilidad de estos profesionales se haga cada vez más grande. Igual que existe ética del diseño hacia un sistema más sustentable medioambientalmente hablando[1136], ¿por qué no podría existir una ética desde el diseño para las libertades y derechos fundamentales de las personas? La filosofía podrá ayudar a los desarrolladores de tecnología. *Tristan Harris*, señaló en un TEDx (2017):

> "Al igual que una ciudad da forma a la vida de sus habitantes, el software da forma a la vida de sus usuarios. Por eso el *software es un dominio de gran responsabilidad*.
>
> - ¿Cómo nos aseguramos de que los diseñadores utilicen el sistema operativo moral más inteligente al tomar decisiones en nuestro nombre?
> - ¿Cómo distinguen entre lo que es bueno para los negocios y lo que es bueno para la sociedad, o incluso para navegar estas situaciones con claridad?
> - ¿Cómo alineamos sus objetivos de diseño con nuestros objetivos de cómo queremos vivir la vida?
> - ¿Cómo captan y minimizan las externalidades sociales y de comportamiento negativas no intencionadas?
> - ¿Cómo podemos responsabilizar a los diseñadores por su influencia sobre las elecciones de las personas?"

En *Center for Human Technology* están creando *estándares de diseño humano* , políticas **y** modelos de negocios que se alinean más profundamente con nuestra humanidad y con la forma en que queremos vivir[1137]. Es importante que aprendamos a partir de nuestra propia práctica de diseño, pero

---

[1136] La ética del Diseño: Hacia un sistema más sustentable y responsable. *Conference: 3er. Congreso Internacional de Bioética*, At Toluca, Estado de México. Recuperado de https://www.researchgate.net/publication/274638707_La_etica_del_Diseno_Hacia_un_sistema_mas_sustentable_y_responsable?enrichId=rgreq-c4338b7ff3468407ed016a5be2e5facd-XXX&enrichSource=Y292ZXJQYWdlOzI3NDYzODcwNztBUzoyMTU3Mzg2MDc1MDk1MDRAMTQyODQ0NzUwMDkyOQ%3D%3D&el=1_x_3&_esc=publicationCoverPdf

[1137] Vid. http://humanetech.com/problem#the-way-forward

también que saquemos lecciones de la historia, las ciencias suaves de la sociología, la antropología y la psicología, y por supuesto, la metafísica y la filosofía[1138].

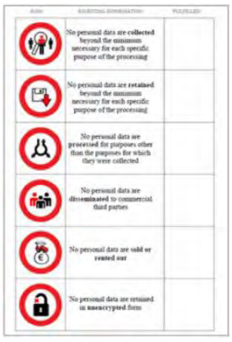
Pero si hablamos de ética del diseño, tenemos que hablar de diseño legal aplicado a las Administraciones Públicas (ciudadanos) y a las empresas (usuarios). Casi el 90% de la información transmitida al cerebro llega por vía visual 60.000 veces más rápido que la textual. Para el ciudadano medio puede resultar complicado entender las extensas políticas de privacidad Por ello, existe un sector de investigadores y expertos de la privacidad que buscamos soluciones que faciliten la comprensión del lenguaje rígido jurídico y puedan entender cuál es la finalidad de sus datos personales. Por ello, se piensan en iniciativas basadas en viñetas, audio guías, videoclips, iconografía, chatbots con asistentes virtuales, etc.

A continuación, se muestra un ejemplo de cómo el diseño legal puede ayudar a entender qué se hace en investigación de salud y las implicaciones legales (extendiéndose incluso al ámbito de la protección de datos).

Fuente: Marietje Botes. Phd thesis. Panelfit en la UPV/EHU (junio 2019). Presentación de Mariana Rissetto y Marie Catherine Wagner.

En cualquier caso, lo ideal sería que se pudiera crear un código de conductas aplicado al sector en cuestión (por ejemplo, en investigación biomédica o ensayos clínicos) donde se informara con iconografía acerca de la finalidad de los datos, de los terceros, del cifrado, de la portabilidad, y de la compensación económica (si la hubiera, en caso de proyectos de interés privado , no público).

[1138] Vid. https://planetachatbot.com/el-papel-de-la-%C3%A9tica-del-dise%C3%B1o-y-las-consecuencias-imprevistas-del-2017-33190df0637



Fuente: Borrador Nuevo Reglamento Europeo de Protección de Datos . LIBE.

Ya hace una década, el Ministerio de Justicia creó una Comisión para la modernización del lenguaje jurídico. Quizás la idea podría aproximarse a :

Fuente: Jorge Morell

Además, se deberá tener especial atención con colectivos vulnerables o desprotegidos, como podrían ser las personas con barreras de accesibilidad sensorial (sordomudas), por ejemplo, a través de *diseño universal* destacando colores en las letras y con ilustración [1139].

4.7. Los valores y la ética de datos.

Los valores son "aquellas conductas que perfeccionan al individuo como persona, a la empresa como organización de personas, y a la sociedad como comunidad de personas" (Deres,17)[1140].

[1139] Isolera, Humberto. Congress of the Europe Deaf Teach, 15 th June, Madrid.

[1140] *Supr cit.* Los principios éticos garantizarán la libertad y dignidad de la persona, y se pueden clasificarse principalmente en (i) el principio de autonomía (respetar la libertad de los otros); (ii) el

Cuando hablamos de valores en las organizaciones podemos referirnos a los valores tradicionales como el logro, la productividad o a los nuevos como el respeto por los derechos humanos, la sostenibilidad, la solidaridad, etc. La evolución del paradigma de los valores en las organizaciones en las últimas décadas ha ido cambiando y se podría resumir con el siguiente cuadro:

	1960-2000 (Elexpuru y Yániz, 2010)	**2000-2020**
"Visión recibida"	*"Visión colaborativa"*	*"Visión global"* (podría denominarse)
Periodo de organización industrial	Nueva organización de la nueva economía. Énfasis intergrupal	Cultura ética corporativa, best practices, RSE.
Autocracia, jerarquía	Valores tradicionales: logro, productividad	Valores nuevos: respeto por los derechos humanos, innovación , sostenibilidad.

Tabla 54. Evolución de los valores en empresa.

Las organizaciones pueden trabajar en los *valores humanos y en los derechos y libertades de las personas*, como son la *privacidad y la protección de datos personales por medio de formación y capacitación*. La protección de datos es un derecho fundamental de las personas que tendrá que ser protegido por las organizaciones poniendo su punto de mira no sólo en los *usuarios, clientes, consumidores o pacientes* sino también en los *empleados* de éstas organizaciones.

Por ejemplo, ¿Por qué no *integrar* dentro del valor de privacidad los valores y derechos novedosos que incluye la nueva LOPDGDD española? Me refiero, por ejemplo, a la transparencia, intimidad y usos dispositivos en el ámbito laboral, al derecho de desconexión digital en el ámbito laboral, etc.

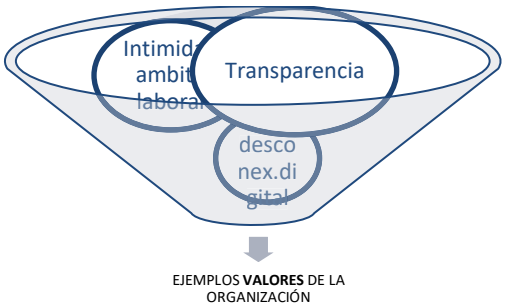


Imagen 85. Posibles elementos integradores de los valores en las organizaciones.

principio de equidad (considerar la igualdad de oportunidades para ser autónomo) y; (iii) el principio de beneficencia (o de "hacer el bien").

El mayor reto no estará tanto en el diseño de los valores sino más bien en su puesta en práctica[1141]. Por tanto, el *liderazgo ético* desde la cúspide y los altos mandos de las organizaciones es fundamental y enfocado a la gestión del cambio. Los líderes de las organizaciones podrían establecer los siguientes pasos para lograr buenos resultados gracias *a los valores*: (i) *Autoevaluación* y medición de su cultura ética y comportamiento organizacional; (ii) Desarrollo de formas *nuevas de liderazgo* apoyándose en los mandos intermedios; (iii) Diseño de *herramientas* para la toma de decisiones **y** responsabilizar a los colaboradores de su uso efectivo y consistente; (iv) *Simplificar* políticas y procedimientos que conecten con los colaboradores (demasiadas reglas no ayudan); (v) *Innovar* en la formación (no sólo anual) sino innovar con *coaching,* por ejemplo.

El estudio de *LRN Ethics & Compliance Program Effectiveness Report* (*2016)* [1142], recoge la opinión de más de 550 expertos legales en *compliance* y utiliza un Índice de Efectividad de *Compliance* (PEI) para medir resultados respecto de *tres áreas críticas* del comportamiento organizacional: (i) *"Decisiones éticas:* Si las decisiones que toman los empleados se encuentran basadas en valores o simplemente conveniencia; (ii) *Justicia organizacional:* Si altos ejecutivos y empleados más exitosos son evaluados con los mismos estándares de conducta que otros empleados; (iii) *Libertad de expresión*: Si los empleados se sienten cómodos para alzar su voz y contribuir libremente al intercambio de ideas"[1143].

Mención especial merecen los valores de la *transparencia y confianza* (consecuencia de la primera). Según *Tranberg y Hasselbach* (2019, 58) "no podemos

[1141] Los altos mandos deberán ocuparse de mostrar los beneficios prácticos que produce el ejercicio de estos valores, no siendo recomendable asumir que se trata de algo obvio. La metodología más eficiente para el fomento de valores es desde principio del refuerzo positivo, el cual pone énfasis en reforzar las buenas prácticas y las conductas que mejor reflejan la cultura organizacional deseada. Las amenazas y los castigos, en el mejor de los casos, sólo logran generar temor, pero no convicción. Se debería buscar una suerte de "recompensa" o "premio" o "elogio" como respuesta a su ejercicio.

[1142] Vid. https://content.lrn.com/research-insights/2016-e-c-program-effectiveness-report

[1143] Utilizando un marco basado en comportamientos en lugar de un *checklist*, el estudio de demostró que las empresas con más altos estándares de comportamiento ético son aquellas que han colocado los *valores* al *centro de sus organizaciones*. De las empresas con mejor rendimiento, dos tercios se enfocan *más en valores que en reglas*. De hecho, en el 90% de dichas empresas sus valores han pasado a formar parte de su estrategia de posicionamiento de marca. Para el 70%, los valores se han convertido en un marco de referencia para la toma decisiones. El estudio de LRN muestra que las compañías en que existe un proceso de toma de decisiones basado en *valores,* son mucho más efectivas, cumplen mejor las expectativas y presentan mejor comportamiento que aquéllas en que rige solo un listado de reglas y decenas de políticas y controles.

entender la privacidad como una *cuestión de confianza,* sólo como una cuestión de protección, cumplimiento y carga administrativa. La forma en que abordamos y manejamos los datos personales y la privacidad es un indicador básico de confianza".

Aunque el investigador italiano *Alessandro Acquisti* hace una segunda y curiosa lectura acerca de la *transparencia* y es que, por sí misma, puede provocar que los usuarios "sospechen" (o al menos, reflexionen sobre dicha transparencia). Según él, "los controles exhaustivos habían llevado a la gente a "compartir más información delicada con un público más amplio. La transparencia y el control son palabras vacías que se usan para trasladar al usuario la responsabilidad por los problemas que otros están creando"[1144]. Por tanto, según este investigador y a raíz de su trabajo "Trampas de la privacidad", la transparencia puede ser beneficiosa para las organizaciones aunque no tanto para los usuarios confiados que comparten más datos personales (y delicados) que con otras que no los tienen el mismo nivel de confianza del usuario[1145].

4.8. La privacidad como valor.

En EEUU, las *compañías de seguros* "monitorean" a los clientes y sus datos para evaluar su salud y el comportamiento para ajustar las correspondientes primas de seguro y para reducir las reclamaciones por daños en sede judicial. ¿Es ético desde el punto de vista de la privacidad? Las aseguradoras justifican sus acciones en el beneficio social de predecir, por ejemplo, por medio de *big data*, las enfermedades futuras. Según el CEO de la aseguradora de salud, Sanitas, la deontología en la relación con el paciente y la reputación de la empresa es lo más importante. En sus palabras señaló "no podemos permitirnos hacer un uso inadecuado de los datos del paciente". Este directivo aboga por

[1144] Vid. https://elpais.com/tecnologia/2013/04/10/actualidad/1365620520_279623.html

[1145] No obstante, si los usuarios entienden que se trata de una falsa transparencia, tal y como establecen *Tranberg y Hasselbach* (2018, 69) se les podría considerar como "charlatanes digitales" *(privacy charlatans).* Se les denomina como tal a "las compañías que prometen a los clientes un cierto grado de privacidad y protección de datos que en realidad no pueden entregar debido a su tecnología, modelo o política de negocio". Para los charlatanes digitales, la privacidad es una estrategia de marketing que si no cumple derivará en grandes consecuencias para su reputación. Así por ejemplo, *Facebook* podría correr el riesgo de convertirse en eso si finalmente no se lleva a cabo la función *"Clear History"* que ha lanzado como control para usuarios sobre la información qué obtiene *Facebook* en otras aplicaciones y web. Vid. https://www.elespanol.com/economia/empresas/20190128/facebook-lanza-centro-recursos-privacidad-empresas/371963142_0.html

el por el acuerdo entre aseguradora y paciente con reglas explícitas y conocidas por ambas partes durante una serie de años[1146] [1147].

La *ética y la privacidad digital*[1148] han sido nombradas como una de las diez *tendencias* tecnológicas estratégicas más importantes para la consultora *Gartner* en el 2019[1149]. Las organizaciones empresariales que ya han comenzado a darse cuenta de esta *cultura ética de la privacidad* -si se puede denominar así-, apuestan por invertir en ello. Contar con una cultura de privacidad promovida por organizaciones puede convertirse, a mi modo de ver, en una *ventaja competitiva* respecto a los competidores, clientes, proveedores, y sociedad, en general. Se ha creado una especie de tendencia o de sector "de moda" donde nuevas empresas con componente tecnológico apuestan por medidas técnicas de seguridad o por el uso del disruptivo protocolo de *blockchain* y los sistemas DLT. No sólo es motivada por la propia responsabilidad social empresarial[1150] sino que todo ello tiene un componente económico detrás.

La privacidad es "una importante *área estratégica* que va mucho más allá del mero cumplimiento con la ley, convirtiéndose en un valor social y una responsabilidad social fundamental" (*Baberger y Mulligan*, 2010)[1151]. En este sentido, si existe la "ética de los negocios" (*business ethics)* que da respuesta a conflictos que afectan a la empresa y los grupos de interés *(stakehonders)* y que asiste a la toma de decisiones, ¿por qué no crear una suerte de "ética de los datos de los negocios y la privacidad"? Pero, a mi modo de ver, y tal y como establece *Colmenarejo* (2017), debería de tratarse de una "disciplina diferenciada" de la actividad propia de las empresas. La autora señala que "los buenos hábitos conforman el carácter y con ello, la moral de las personas, las

[1146] Bamberfer, K., Mulligan, D. (1 de enero de 2010). Privacy on the books and on the ground. *Berkeley Law Scholarship Repository*. Recuperado de https://www.technologyreview.es/s/10266/no-podemos-permitirnos-usar-inadecuadamente-los-datos-del-paciente

[1147] Gracias a la información que se recopila (página web, apps, etc) los pacientes entran en programas de salud preventivos (100.000 programas en 2017) para patologías crónicas, como diabetes o hipertensión o planes de estilo de vida, por ejemplo, de preparación física o de nutrición

[1148] Ahora bien, pensemos en la parte oscura: ¿la privacidad y protección de datos pondrá *límite a la innovación de la Industria? ¿se convertirá la cultura corporativa de privacidad y protección de datos en una nueva moda de inversión por parte de las empresas?* La idea de que la protección de datos es una limitación a la innovación o progreso digital ha sido un tema recurrente desde hace años en el contexto empresarial digital, hasta el punto de que el propio legislador comunitario ha venido insistiendo en la posible convivencia de ambas.

[1149] Vid. https://dataethics.eu/en/data-ethics-is-a-game-of-interests/

[1150] Ya en el capítulo 6 ("Ética y responsabilidad") hablábamos de la responsabilidad social corporativa como una aplicación voluntaria de sus principios para favorecer la reputación y confianza de consumidores y proveedores refiriéndonos a la concepción más utilitarista de la ética de los negocios.

[1151] *Supra cit.*

buenas prácticas deberían conformar una cultura". Podríamos tratarla como aquella disciplina que comprende los aspectos de la conducta de los negocios (tanto las conductas individuales de las personas de la organización como la organización en su conjunto) respecto a la forma de almacenar, gestionar y utilizar los datos de las personas.

Los datos son un activo con un componente eminentemente de "riesgo" para la Industria en sí. El riesgo del que hablamos se refiere a la incertidumbre o amenaza mediante una secuencia de actividades debido al impacto de las nuevas tecnologías en los derechos y libertades de las personas o titulares de derechos[1152]. Y es que según *Tranberg y Hasselbach*[1153], "en el modelo de negocio digital más común de la actualidad, los consumidores pagan productos *gratuitos* con sus datos personales".

El profesor Puyol (2018) [1154], en su artículo sobre "la ética y la responsabilidad derivada de los algoritmos" señala que "a los efectos de controlar y mitigar el impacto que el uso de los algoritmos tiene para la sociedad, cabe plantearse desde el ámbito de las empresas y los desarrolladores las siguientes preguntas: *"¿El uso de los algoritmos está dentro del ámbito de la responsabilidad social corporativa y empresarial? ¿Los valores y los principios que informan esta materia, deben ser contemplados sobre esta óptica, en primer término, y no como una simple responsabilidad civil, o en su caso de Compliance?"*

En mi opinión, desde un punto de vista etimológico el uso ético (o "correcto") de los algoritmos estaría dentro de la disciplina de Responsabilidad Social Empresarial si la organización está desarrollando un conjunto de "actividades" (medidas, políticas, principios u otras herramientas) materializadas en códigos éticos o no. Cuando nos referimos

[1152] Las empresas e instituciones que consideren contener estos riesgos deberán tener los procesos de gestión adecuados con las siguientes etapas diferenciadas: identificación de amenazas, evaluación de riesgos y tratamiento de riesgos. El RGPD focaliza su atención en las amenazas sobre los derechos y libertades de los interesados (AEPD, Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD. Ver en: https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf)

[1153] *Supra Cit.* pp 13.

[1154] Vid. https://confilegal.com/20181223-la-etica-y-la-responsabilidad-derivada-del-uso-de-los-algoritmos/

4.9. Casos de estudio

Hablemos de algunos casos que hablan las autoras Tranberg y Hasselbach a lo largo de su trabajo:

i. Caso de Clue.

La pista de seguimiento de la fertilidad, con sede en Berlín, ayuda a monitorear la fertilidad y proporcionan nuevos conocimientos para la reproducción y la investigación en salud. Clue es consciente de que tratan con datos sensibles, por lo que la política de privacidad de la empresa es comprensible. Es posible utilizar la aplicación sin necesidad de un cuenta. Los usuarios también pueden crear una cuenta - los datos de los cuales serán *anonimizados para investigación clínica y académica* - y usar sus datos para obtener datos visualización y creación de predicciones sobre el propio ciclo. Los datos del mismo ciclo se almacenan por separado de la información personal, lo que asegura una capa extra de anonimato.

ii. Caso Data for Good Foundation.

La Fundación busca proporcionar una plataforma para reunir a las personas de la salud, las lesiones y la información pertinente sobre el comportamiento, y vincularla con datos sociales como la educación, el empleo, el peso, la edad, residencia, pasatiempos y datos de *automedición* aplicables, tales como presión arterial, sueño y pasos al día. Todos estos datos serán accesibles y controlables por el individuo para mejorar su calidad de vida. estilo de vida. Los seguros y fondos de pensiones, municipios, los investigadores y otros terceros sólo tienen acceso a los datos en una forma anónima. La Fundación espera, por tanto, *garantizar la microtarifa*, es decir, que el cálculo de las primas para los individuos se haga éticamente.

iii. Caso de F-secure y Qwant.

La nube no estadounidense los servicios están empezando a afianzarse como buscadores diferentes a Google.

iv. Caso de Cozy.

Está comercializando proactivamente como la compañía como "anti-Google".

v. Caso de Microsoft.

En 2012, Microsoft[1155] lideró una feroz campaña contra Google y cuando se supo que Gmail rastreaba contenido en los correos electrónicos para mostrar publicidad personalizada, prometió que los productos

[1155] Cfr. MICROSOFT (2014a): "Microsoft, en la lista de las Empresas Más Éticas del Mundo por cuarto año consecutivo". Recuperado de https://news.microsoft.com/esxl/microsoft-en-la-lista-de-las-empresas-mas-eticas-del-mundo-por-cuarto-anoconsecutivo/
Desde 2011, la empresa Microsoft viene apareciendo en los primeros puestos del ranking "World's Most Ethical Companies" que elabora anualmente Ethisphere. Este premio reconoce a las compañías que van más allá del simple discurso ético y lo aplican al día a día de sus organizaciones.

de Microsoft Hotmail no harían los mismo y abrió el sitio *Scroogled.com* (ya cerrado en 2013) para burlarse de los métodos de recopilación de datos personales de Google. Más recientemente, sin embargo, Microsoft ha retrocedido en relación con su las promesas de privacidad y la batalla contra Google.

En su Código de Conducta se tratan 3 aspectos, divididos en 5 apartados: Cumplimiento con las leyes, regulaciones y políticas de Microsoft, administración y protección de la información, trabajo responsable y servicio a las comunidades de todo el mundo, fomento del dinamismo y la diversidad en el entorno de trabajo y administración responsable de los activos

vi. Caso de Apple

Se está esforzando por diferenciarse del resto de gigantes desarrollando su privacidad e incluso emitiendo declaraciones públicas contra el gobierno de EEUU. Así por ejemplo, Apple negó la petición del FBI de descifrar sus propias características de seguridad para acceder a los datos en el iPhone de un terrorista. Y aprovechó el CES de Las Vegas para publicitar "lo que sucede en tu iPhone, permanece en tu iPhone":

Imagen 86. Panel publicitario de la marca Apple respecto a la privacidad: Ymedia

Imagen 87. Anuncio Apple 2019 campaña privacidad. Fuente: Youtube.

Como decíamos la transparencia debe llegar al público aunque *Apple* deberá ser cuidadoso sino quiere caer en el error de ser un charlatán de la privacidad.

vii. Caso de Tinder.

En abril de 2016, *Swipebuster.com*[1156] fue tras Tinder y expuso a sus usuarios que podrían averiguar si su jefe, novia o otros usan esa aplicación. Esta compañía no hackearía a Tinder, sino buscaría en las bases de datos que la API oficial de Tinder que pone a disposición de los desarrolladores de terceros. El objetivo de *Swiperbuster* era llamar la atención el hecho de que las empresas no informaran a los usuarios cuando los datos están *disponibles para otros.*

[1156] Vid. https://www.ticbeat.com/cyborgcultura/swipe-buster-la-pagina-que-comprueba-si-tu-pareja-esta-en-tinder/

4.10. Conclusión: "De las reglas a los valores, de la amenaza a la identidad corporativa".

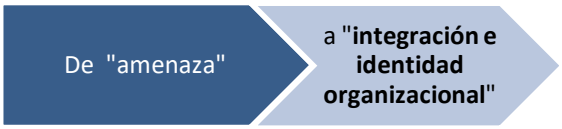
En el escenario disruptivo de las tecnologías emergentes y de la cuarta Revolución Industrial se ha propiciado un periodo de enormes desafíos. *Dov Seidman,* invitado en 2004 a la *U.S Sentencing Commission* y CEO de LRN[1157], compañía de consultoría sobre educación de ética y cultura corporativa de organizaciones, protección de datos y otras cuestiones, señaló que "las empresas deben pasar de un enfoque meramente formal de *checklist* a realmente promover culturas éticas y buen comportamiento".

En nuestro contexto, las organizaciones asumirán actividades o comportamientos que posibilitarán la convivencia y el bienestar de la comunidad y la sociedad, promoviendo colaboración entre los *stakeholders,* como pacientes, usuarios o consumidores de *e-health*, clientes, administraciones públicas, industria farmacéutica, universidades, gobierno, aseguradoras de salud; pero además creando un entorno favorable para el desarrollo de la organización empresarial. En concreto, "las organizaciones de hoy deben responder a un hecho más allá de lo económico, de allí que en su misión y visión es importante destacar un futuro sustentable a través de un sistema de valores, creencias, actitudes, hábitos, normas y políticas, donde identifican su personalidad y destino en el logro de sus fines económicos y sociales" (Franco de Franco *et al.,* 2010) [1158].

Pero es fundamental que se supere la concepción amenazadora de los mismos para alcanzar una *concepción integradora y de identidad organizacional* para todos los miembros de la organización, e incluso, del resto de *stakeholders*.

[1157] Vid. http://cdn2.hubspot.net/hubfs/319387/LRN_GCL_Brochure.pdf

[1158] Franco de Franco, M.J.; Perdomo, Y. C; Godoy, E. (2010) Preeminencia de la Ética sobre la Tecnología *Revista Daena . Revista Internacional de Buena Conciencia.* vol. 5 Número 1, p81-97. 17p.Recuperado de http://www.spentamexico.org/v5-n1/5(1)81-97.pdf



En definitiva, es fundamental no poner el foco *únicamente* en los aspectos superficiales de *gobierno corporativo* como son las reglas, las regulaciones, los requisitos, los *checklists*, las políticas y los procedimientos, sino que para obtener el mejor resultado, la organización se enfoque en su objetivo empresarial, en el respeto, en la capacidad de crear confianza en la creciente interdependencia, así como en el *compromiso con valores*[1159].

5. LA ETICA DE LOS DATOS Y LAS INSTITUCIONES PÚBLICAS Y GOBERNANZA.

El supervisor europeo de protección de datos, *Giovanni Butarelli,* ha señalado recientemente que "el *mapeo digital es* un conglomerado de puntos de datos únicos, mal interpretados en un retrato digital, una caricatura en la que se toman decisiones sobre y para nosotros". Además, advirtió que "la *creación de un extenso perfil digital*, como la base de la percepción e interacción del Estado con cada uno de sus ciudadanos, plantea una serie de preguntas éticas; (i) la tecnología digital promete que las personas puedan verificar su identidad para obtener los beneficios a los que tienen derecho, ¿pero estas personas tendrán el control de sus nuevas identidades digitales? (ii) ¿es correcto que su capacidad para participar en una sociedad digitalizada dependa de una serie de medidas corporales?; (iii) ¿deberíamos reducir nuestro yo digital a los perfiles desarrollados por terceros que, a su vez, determinan la información 'personalizada' que vemos en nuestras redes sociales y los productos que se nos presentan en las plataformas de comercio electrónico? ; (iv) ¿pueden los aspectos confiables de nuestras vidas crear una imagen representativa de quienes somos? [1160]. *Butarelli,* ante estos interrogantes, concluye que "la

[1159] Vid. https://es.weforum.org/agenda/2017/05/por-que-las-organizaciones-mas-exitosas-se-enfocan-en-valores/

[1160] Tal y como advirtió Butarelli; "el gobierno de la India ha estado implementando en los últimos años Aadhaar, un mecanismo para administrar servicios a la población a través de un número de identificación basado en los datos biométricos y demográficos de más de mil millones de

tecnología de *big data* no debe estar habilitada para crear suposiciones sobre nosotros y tomar decisiones sobre ellos; esta es la razón por la cual la protección de datos y los derechos de privacidad son esenciales para preservar la dignidad humana en el mundo de hoy"[1161].

5.1. Respecto a la gobernanza colaborativa, gestión de datos de la salud y privacidad.

El "modelo Salus".

Se ha pensado en la creación de un modelo de ciudadanía (*modelo Salus,* en adelante) donde se permita que los ciudadanos compartan datos colectivamente acelerando la investigación e innovación en la atención sanitaria, compuesto por tres grupos principales de actores:

(i) Los c*iudadanos*: los propietarios legales de sus datos de salud, que se almacenan en varias bases de datos;

(ii) Los *poseedores de los datos:* los propietarios de las bases de datos donde se almacenan los datos de salud de los ciudadanos. Algunos datos potenciales de salud pública y privada, los centros de salud inteligentes y los empresas de dispositivos (vestibles, aplicaciones);

(iii) *Usuarios de los datos:* las partes interesadas en acceder al datos para diferentes fines. Entre los posibles destinatarios se incluyen investigadores, empresas y administraciones públicas.

La Administración Pública se puede plantear los algunos interrogantes como por ejemplo los planteados en el proyecto *Salus Coop*. (2016)[1162];

"¿Es posible involucrar más a los ciudadanos activamente en la toma de decisiones proceso relacionado con el uso de sus datos de salud? ¿Qué tipo de modelos de gobernanza puede ser desarrollado para dar a los ciudadanos la propiedad y el control de su salud datos? ¿Cómo podemos fomentar el intercambio de datos que beneficia a los

---

personas. El esquema teóricamente voluntario se expandió rápidamente a una multiplicidad de otros servicios, como pensiones, matrículas escolares, ley de empleo rural e incluso cuentas bancarias y números de teléfonos móviles, lo que atrajo fuertes críticas por muchos motivos, incluida la privacidad y la inclusión social en función de la presentación. a la tecnología de vigilancia".

[1161] Vid. https://www.ourworld.co/humanitys-finest-work-of-art/

[1162] Vid. https://static1.squarespace.com/static/57c55d71725e25ba4eb91756/t/58e533fb1b631bedcc67acad/1491416088875/Salus+coop.pdf pag. 9

ciudadanos, la salud profesionales, investigadores, profesionales de la salud proveedores y empresas dispuestas a ofrecer servicios/productos?"

En el estudio realizado han sacado como conclusión: cuatro principios fundamentales que deberían ser se consideran los pilares de toda gobernanza dirigida por los ciudadanos para la gestión de datos de salud:

(i) *Donación condiciona:* Los ciudadanos tienen derecho a decidir en virtud de la cual condiciones en las que quieren donar sus datos de salud. Los ciudadanos quieren saber quién utilizará sus datos personales y para qué;

(ii) *Beneficio colectivo:* El sistema necesita asegurarse que el uso de los datos tiene un claro e inequívoco beneficio para la sociedad;

(iii*) Incentivos*: Como incentivos en forma de servicios, descuentos, etc.;

(iv) *Gestión de derechos*: gestión de condiciones establecidas por los miembros de la cooperativa, las credenciales para acceder a los datos y las solicitudes de los receptores de datos que deben cumplir los principios establecidos en la cooperativa.

¿Cuáles serían los papeles más importantes de los ciudadanos en este escenario? (Salus Coop, 17)[1163]:

Papel de los ciudadanos	**Características**	**Ejemplos**
Pacientes informados (y con consentimiento)	Se les pide su consentimiento para donar sus datos a investigaciones públicas	**Visc+** (Catalunya) Cara.data (UK) Genome Project (Estonia)
Contribuyentes	La gente proactivamente decide donar sus datos de salud , también a plataformas	DataDonors Open Humans
Consumidores	La gente comparte datos con compañías quienes les brindan con dispositivos de salud, aplicaciones o servicios	PHR apps (e.g. Microsoft HealthVault) Wellness Apps and other devices (Fitbit, Garmin, etc.) Personal service (e.g.

[1163] ¿Cómo organizar todo ello? (*Salus Coop*, 39-42).Las relaciones entre las partes están vinculadas por un conjunto de *acuerdos contractuales* que esbozan los principios éticos comportamiento, intercambio de valor, estándares tecnológicos, términos de uso de los datos, etc., con lo que las partes deben estar de acuerdo. Así por ejemplo, uno de los acuerdos es el acuerdo ético que define los objetivos de la cooperativa y los principios éticos que todos las partes se comprometen a respetar. Destacan dos dimensiones importantes: la transparencia y participación. El acuerdo ético funciona como una declaración y, por lo tanto, no es jurídicamente vinculante. Sin embargo, las partes implicadas pueden considerar a alguna parte como responsable de incumplimiento. Pero además, tal y como señalan "algunas dimensiones éticas están incluidas en los demás contratos jurídicamente vinculantes firmados por los participantes".

		23andMe)
Prosumer	A las personas se les proporciona herramientas que les permiten estar involucrado en la investigación. Por ejemplo, pueden proporcionar información sobre su enfermedad a través de herramientas de redes sociales. (Ej. PatientsLikeMe)	Social networking services: e.g. Patientslikeme
Partners	La gente está informada sobre el uso de sus datos y puede participar en la toma de decisiones procesos de fabricación.	HealthBank Midata.coop OHDC

Tabla 55. Papeles importantes de los ciudadanos en la gestión colaborativa y los datos de salud en la sociedad.

5.2. Especial mención a la gobernanza y a las investigaciones científicas con big data.

En el contexto de las consideraciones éticas y legales de incluida la recopilación de datos, el acceso, la liberación y el enlace, análisis, reutilización, etc., en los siguientes elementos se consideran cruciales para dicho marco[1164].

- Procedimientos para el consentimiento (amplio), el nuevo contacto (incluida la devolución de los resultados) y consentimiento.
- Procedimientos para la disidencia, como alternativa al consentimiento.
- Disposiciones para garantizar los derechos de acceso, rectificación y cancelación de datos.
- Políticas después de la muerte de un participante.
- Disposiciones sobre la propiedad de los datos y los productos derivados de ellos.
- control de calidad y protecciones para proteger la privacidad y la confidencialidad.
- Disposiciones sobre cómo se tratarán los datos en caso de cambio de propiedad o cierre de la base de datos.
- Transparencia de los algoritmos utilizados para el reconocimiento de patrones; arreglos para verificar el perfil de individuos o grupos de acuerdo con consideraciones éticas.
- Divulgación de interés comercial y colaboración con partes comerciales.
- Arreglos que permiten a los participantes mantenerse informados sobre la novedad actual y novedosa uso de datos, incluidas las actividades de investigación.
- Una política clara sobre la divulgación de resultados de investigación individuales y agregados a Participantes.

[1164] *Supra cit.* Informe ICB Unesco.

- Disposiciones para la participación de los participantes en el diseño de la gobernanza procedimientos, en particular con respecto a la supervisión ética y la comunicación con proveedores de datos. Solución : blockchain
- Arreglos para compartir los beneficios. Solución : blockchain
- Disposiciones relativas a las poblaciones indígenas / locales y las minorías tradicionales.
- Niños y adolescentes que alcanzan la edad de madurez durante la investigación proyecto debe tener la oportunidad de dar su consentimiento informado para el almacenamiento y uso continuo de sus datos, y también deberían poder retirar consentimiento para futuras investigaciones. Solución : blockchain e identidad digital.

5.3. Respecto a la preocupación de los Hospitales públicos: La ciberseguridad.

Especialmente inquietantes son las investigaciones de *Billy Rios* sobre las vulnerabilidades de seguridad en hospitales en bombas de infusión de fármacos de la empresa Hospital (que ha instalado 400.000 bombas en el mundo) donde el ciberdelincuente podría controlar remotamente la cantidad de fármacos que administran al paciente[1165], sin que se emita una alarma, poniendo en riesgo la vida del paciente. Todo ello porque los atacantes no necesitarían acceso físico a la bomba dado que los módulos de comunicación estaban conectados a las redes de los hospitales, que a su vez están conectadas a Internet.

Imagen 88. Bombas de infusión de medicamentos en Hospitales. Fuente: Wired. Billy Rios

Barnaby Jack[1166], uno de los profesionales de la seguridad más renombrados[1167]. En 2012, su testimonio llevó a la Administración de Drogas y Alimentos de los Estados Unidos a cambiar las regulaciones con respecto a los dispositivos médicos inalámbricos. Es conocido por investigar las vulnerabilidades en el sector sanitario. En el 2011, demostró por primera vez el pirateo inalámbrico de las

[1165] Vid. https://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps/
[1166] Vid. https://en.wikipedia.org/wiki/Barnaby_Jack
[1167] Vid. https://www.eldiario.es/hojaderouter/seguridad/Black_Hat-Def_Con-hackers-hacking-las_vegas_0_276122639.html

bombas de insulina[1168]. En 2012, demostró la capacidad de asesinar a una víctima pirateando su marcapasos.

También, los investigadores Billy Rios de WhiteScope y Jonathan Butts de QED[1169] Secure Solutions demostraron cómo los atacantes podían instalar remotamente un firmware malintencionado en un dispositivo utilizado por los médicos para controlar los marcapasos de sus pacientes. Esto se debe a la falta de cifrado en el proceso de actualización del *firmware de Medtronic*. Además, también con ataques de ciberseguridad se pueden falsear signos vitales[1170] de pacientes.

Recientemente, han salido a la luz investigaciones[1171] donde se ha descubierto la existencia y viabilidad de malware que a través de IA puede "manipular" las imágenes médicas como radiografías oncológicas. Esto significaría que podría añadir elementos en las imágenes que hicieran adoptar un diagnóstico erróneo, o eliminar los elementos o nódulos cancerígenos imposibilitando el diagnóstico correcto y su tratamiento oportuno.

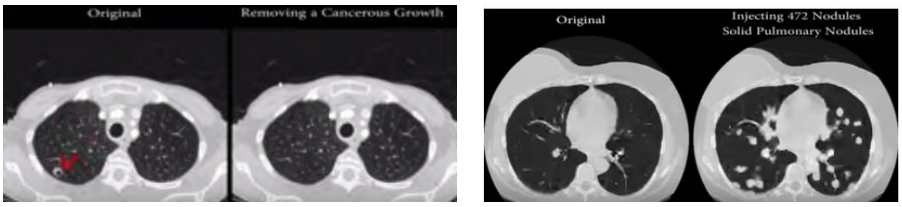


Imagen 89. Pantallazos de manipulación de diagnóstico y el malware. Fuente: Cyber Security Labs Ben Gurion University

El Washington Post[1172], ha anunciado hace poco que una coalición formada por hospitales y fabricantes de dispositivos médicos respaldada por el gobierno.

[1168] Stilgherrian (21 de octubre de 2011). "Hackeo de dispositivos médicos letales llevado al siguiente nivel" . CSO Online (Australia) . Recuperado de . https://www.cso.com.au/article/404909/lethal_medical_device_hack_taken_next_level/

[1169] Vid. https://www.blackhat.com/us-18/briefings/schedule/#understanding-and-exploiting-implanted-medical-devices-11733

[1170] Vid. https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/80-to-0-in-under-5-seconds-falsifying-a-medical-patients-vitals/

[1171] Vid https://arxiv.org/abs/1901.03597 y https://www.youtube.com/watch?v=_mkRAArj-x0

[1172] Vid. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/01/29/the-cybersecurity-202-medical-devices-are-woefully-insecure-these-hospitals-and-manufacturers-want-to-fix-that/5c4f4a661b326b29c3778cef/?utm_term=.f7488baac1fb. Y es que según *Greg García*, director ejecutivo del Consejo de Coordinación del Sector de la Salud, hay 4 motivos por los que la seguridad no llega a los hospitales. En primer lugar, las regulaciones proteccionistas dificultan que los fabricantes de dispositivos lleguen a los sistemas hospitalarios que mantienen esa información para *parchear y actualizar su software* con nuevas protecciones. En segundo lugar, *los hospitales a menudo no están equipados* para parchear los dispositivos en sí mismos, porque carecen de efectivo (los hospitales más pequeños no pueden pagar a los jefes de

han publicado un plan de seguridad conjunto[1173]. Y es que el hecho de que los hospitales públicos no se le apliquen sanciones hace que la conciencia de privacidad, protección de datos, en general, y las medidas de seguridad técnicas y organizativas, en particular.

seguridad de la información). En tercer lugar, muchos dispositivos médicos, como las máquinas de resonancia magnética, están diseñados para durar una década o más, lo que significa que incluso si se crean teniendo en cuenta la ciberseguridad, se enfrentarán una nueva generación *de amenazas de piratería* al final de su vida. Finalmente, los piratas informáticos criminales que comenzaron a atacar la atención médica son más tardíos que otros sectores, como los servicios financieros, donde la información robada podría convertirse más rápidamente en efectivo. Sin embargo, cuando llegaron, entraron en vigor.

[1173] Vid. https://healthsectorcouncil.org/the-joint-security-plan/

CONCLUSIONES

A continuación para conseguir un orden deseable en la exposición de 36 conclusiones, recuperaremos las preguntas de investigación (reflejadas en el marco teórico) y procederemos a la desarrollo de las conclusiones enumeradas según la temática. Por último, se apuntarán dos líneas de investigación futuras.

RESPECTO A LA INDUSTRIA DEL CUIDADO DE LA SALUD Y TRANSFORMACIÓN DIGITAL Y CONSIDERACIONES ESPECÍFICAS DE LAS TECNOLOGÍAS.

Preguntas de investigación
1. ¿Qué repercusiones y perspectivas de futuro presentará la Industria en relación con los flujos de información, los datos como activos y la protección de datos? **2.** ¿Qué repercusiones podrían tener en los derechos de los titulares de datos la aparición de aseguradoras interactivas con convenios con empresas tecnológicas que se sirven de éstas últimas para seleccionar clientes "más rentables"? Piénsese en dispositivos Apple Watch y aseguradoras como John Hancok. **3.** Analizar la política de privacidad de una aseguradora interactiva real. Ejemplo: Vivaz . **4.** ¿Tienen control efectivo las empresas respecto a la tecnología que se utiliza? Por ejemplo, respecto a las decisiones automatizadas. **5.** ¿Qué soluciones posibles, a priori, se podrían vislumbrar, respecto a la Industria, la tecnología y el derecho de protección de datos personales?

1. La industria del cuidado de la salud aprovechará al máximo la revolución digital lo que se traducirá en ciertas repercusiones y perspectivas de futuro. En concreto, a mi modo de ver, las *compañías farmacéuticas* no podrán controlar totalmente los datos generados (su activo más valioso) de sus productos o servicios, salvo que interactúen con terceros (pacientes, investigadores, profesionales sanitarios, empresas tecnológicas, universidades, etc.), algo que podrán realizar solo en el contexto de transformación digital. Por otro lado, se encuentran *las aseguradoras (interactivas o virtuales, también)* que *s*eguirán otorgando incentivos o recompensas a las personas que utilicen ciertos dispositivos y ceden sus datos personales. Este es un escenario que despierta gran preocupación por varios motivos a mi modo de ver. Por un lado, en lo que se refiere a transparencia y procedencia de datos personales a través de perfiles abiertos de RRSS. Y por otro, a lo referente a la transparencia y concienciación de la

sensibilidad de los datos de salud como datos de categoría especial que requieren de una mayor protección si cabe.

2. Cuando se trata de seguros interactivos que establece el carácter obligatorio del uso de dispositivos como wearables o apps para el seguimiento y estudio de la condición física y la rentabilidad de los clientes potenciales, se requerirá extremar enormemente las precauciones y la transparencia en la información del alcance del tratamiento de datos y justificar, el empleo de dispositivos siendo proporcional y minimizando los datos necesarios, cumpliendo las obligaciones correspondientes en materia de protección de datos. Es una cuestión absolutamente delicada que requerirá no perder de vista en el futuro de las aseguradoras interactivas con convenios con tecnológicas.

3. Después de analizarlas, sería conveniente dar mayor énfasis al principio de transparencia respecto al apartado de "*procedencia"* ya que, por ej., la aseguradora tomará datos "manifiestamente públicos" como en perfiles abiertos de RRSS. Es extremadamente delicada esta cuestión. Se deberían extremar la transparencia por medio de herramientas concretas (legal design y/o iconografía), detallando qué RRSS y el alcance de la información. Respecto a las decisiones automatizadas y concretamente, al derecho a la oposición del mismo, debería ser más claro, explicando los "arboles de decisión" que motivan determinadas acciones de la aseguradora. Resulta injusto que los potenciales asegurados sean "discriminados" por no realizar X pasos al día, pero sobre todo, cuando no sepan cual es el motivo por el que se le ha descartado al tratarse de "cliente no rentable" tras el tratamiento de sus datos personales de salud. Esta cuestión requiere de estudio, discusión y un abordaje práctico por parte de todos los stakeholders implicados; reguladores, industria, colectivos de asegurados, asociaciones de pacientes, etc.

4. La verdad es que muchas empresas aún no saben cómo están "aprendiendo" las máquinas más complejas por lo que resultará bastante difícil poder explicarlo a los propios usuarios. Prueba de esta pérdida de control por parte del "responsable", se extiende también al legislador, el cual no ha contemplado aún que ocurrirá cuando los sistemas evolucionasen a redes neuronales ("*deep learning")* autónomas que no requieren de intervención humana. El cliente de tecnología X tendrá una doble

obligación; primero, elegir un proveedor de tecnología X, y segundo, asegurarse de que cumpla la normativa en protección de datos para evitar incurrir en responsabilidades.

5. Tras la elaboración de este trabajo, se hace necesario una llamada a la reflexión sobre soluciones jurídicas y tecnológicas que otorguen poder de decisión a las personas y faciliten la transparencia a las organizaciones e instituciones públicas y privadas. Proporcionar un *modelo de autogestión* de la privacidad (SOLOVE, 2013) podría ser una buena solución, unida a otras buenas medidas organizativas y técnicas. Las propias tecnologías podrían posibilitar dicho modelo. Los *datos de salud* como datos de categoría especial son vulnerables por sí mismos dada su naturaleza. No obstante, el valor que generan tecnologías como *Big Data, IA e IoT* hace que no podamos ignorar las ventajas que aportan la mejora de la calidad de la vida de las personas y el desarrollo conjunto de la sociedad.

RESPECTO AL REGIMEN JURÍDICO EN PROTECCIÓN DE DATOS DE CLOUD COMPUTING E IoT DESDE EL ENFOQUE DE LA INDUSTRIA DEL CUIDADO DE LA SALUD DIGITAL.

Preguntas de investigación
6. ¿Cuál es el impacto de cloud en los titulares de datos? **7.** ¿Los contratos de adhesión de cloud protegen a los titulares? ¿qué consecuencias acarrean? **8.** ¿Qué implicaciones conllevan las subcontrataciones de servicios cloud? **9.** En Internet de las Cosas (de la salud) , ¿qué sujetos pueden participar y cuáles son sus responsabilidades?(si las tienen) **10.** Analizar situaciones reales. Ejemplo: App Social Diabetes.

6. Un hospital, un centro de atención primaria, una clínica dental, un laboratorio, una aseguradora son ejemplos de clientes de servicios de *cloud computing* como el almacenamiento de datos. Pero en este caso**,** ¿las personas titulares de los datos almacenados en cloud podrán entender cómo se protege sus datos?, y cuando existan consorcios formados por numerosos responsables (ej. centros sanitarios, aseguradoras privadas, promotores farmacéuticos, investigadores, etc.), ¿sabrán a quién dirigirse para ejercitar sus derechos? En mi humilde modo de ver y tras las investigaciones realizadas será muy complicado si no se cumple de forma efectiva el deber de información y el

principio de transparencia de cada uno de ellos. Los derechos de las personas pueden verse vulnerados.

7. Hay que tener en cuenta que la mayoría de los contratos cloud son con contratos tipo y de adhesión, donde en pocas ocasiones cabe negociación alguna salvo que se traten de clientes grandes (no es el caso de pymes sanitarias, por ejemplo); ¿qué consecuencias puede tener todo ello? La conclusión se sustenta en si no se pueden negociar los extremos de legalidad en protección de datos, nos encontraremos ante evidentes vulnerabilidades de los titulares de datos almacenados en cloud cuando el régimen jurídico sea más laxo que el europeo. Piénsese en proveedores cloud de laboratorios con servidores cloud alojados en China o India.

8. También hay otra realidad que se ha detectado a lo largo de este trabajo y concierne a las subcontrataciones cloud, y tiene que ver con la pérdida de control del titular frente a la cadena de suministro del servicio y el ciclo de vida de sus datos. El proveedor *cloud* subcontrata conforme van surgiendo las ofertas y lo hace en un contexto de continuo cambio. Esto provoca que no pueda ser todo lo transparente que debería. En este sentido, ante contextos dinámicos, soluciones dinámicas. Por ejemplo, por medio de un anexo la lista de todos y cada uno de sus subproveedores en tiempo real resolvería esta opacidad incluidas en la página web del proveedor cloud para que su actualización fuera más sencilla.

9. Pasemos a los servicios de *Internet de las Cosas de la salud.* Identificar los sujetos que participan en la cadena de suministro, hemos visto que tampoco será nada baladí. Por un lado, se encuentran los *fabricantes de dispositivos* (por ejemplo, Fitbit). Un escenario bastante frecuente es la aparición de aseguradoras que realizan consorcios o convenios con tecnológicas y proveedores de salud para *rentabilizar el negocio.* En todo caso, ante estas situaciones y otras donde haya dispositivos IoT de salud, resulta muy importante seguir lo establecido en el RGPD, pero también las recomendaciones del antiguo GT29. Por ejemplo, me refiero a informar del tipo de datos (salud de categoría especial) que son recogidos por los sensores, contar con los medios suficientes para interactuar con subencargados ante solicitudes de titulares, contar con un interfaz a disposición de los individuos con datos agregados y en bruto, tener un protocolo de notificación brechas de seguridad o aplicar el principio de minimización en la recogida de los datos, etc. Por otro, se encuentran los *desarrolladores de API* (por ejemplo,

Medicare o Medicaid) que permiten a los beneficiarios conectar sus datos a las aplicaciones, servicios y programas de investigación en los que confían. Serán responsables en la medida que el acceso a los datos de la API es un tipo de tratamiento, *per se*. Además, están las propias *organizaciones de la Industria del cuidado de la salud* o aseguradoras de salud como clientes y responsables del tratamiento. Piénsese, en *laboratorios farmacéuticos* que piden a desarrolladores el diseño una API para crear una app y que tendrán obligaciones de encargado de tratamiento.

10. Por ejemplo, la app *Social Diabetes* podrá subcontratar a otros desarrolladores o proveedores como RRSS. Especial atención merece esta última cuestión, en el contexto de nuestro trabajo, debido a la escasa concienciación de privacidad de la salud de los individuos y ciudadanía. Aún la población desconoce que aseguradoras interactivas (como la española *Vivaz)* utilizan fuentes públicas como FB (a pesar de que se informe en la política de privacidad). Y es que acaso, ¿el usuario que sube un informe a FB con los resultados de su dispositivo (p.e. *Social Diabetes*) no elige la finalidad de su registro y el modo en que queda registrado? ¿podrían considerarse corresponsables junto con la red social? ¿el individuo es titular y a la vez corresponsable del tratamiento? El GT29 ya señalaba que "los interesados son aún más propensos a hacer uso de las cosas conectadas cuando pueden compartir esos datos públicamente o con otros usuarios". Los responsables y encargados deberán ser totalmente transparentes si quieren acercarse al cumplimiento de la normativa.

RESPECTO AL RÉGIMEN JURIDICO EN PROTECCIÓN DE DATOS DE BLOCKHAIN DESDE EL ENFOQUE DE LA INDUSTRIA DEL CUIDADO DE LA SALUD DIGITAL.

Preguntas de investigación
11. Identificar quiénes son los responsables y quiénes son los encargados del tratamiento de datos personales, subencargados y titulares de datos. **12.** Analizar la forma de asignar responsabilidades a los sujetos jurídicos implicados. **13.** Estudiar cómo podría beneficiar blockchain como gestor de control de acceso y permisos para datos y registros de salud a los titulares de datos personales. **14.** Visto lo anterior, quedaría la parte más importante, ¿hasta qué punto esta tecnología es compatible con el RGPD? (14.1.) ¿será compatible el derecho de rectificación? (14.2.) ¿se podría hablar de posibles exenciones a las obligaciones por motivos de limitaciones técnicas? (14.3.) ¿qué posibles soluciones técnicas podrían existir para aplicar modificar o cancelar datos en los bloques? **15.** Consideraciones prácticas. ¿Qué recomendaciones iniciales podríamos dar a los desarrolladores de blockchain en entornos de salud?

11. Como decíamos, *ésta tecnología* es un sistema descentralizado por naturaleza, y no encaja con el modelo de *dicotomía de responsable/encargado* de tratamiento. No existe un sujeto que se responsabilice del mismo, al igual que no hay un responsable de internet. *Blockchain* es un protocolo más que una tecnología, por lo que intentar determinar quién es el *responsable de tratamiento* resulta materialmente difícil, pero me aventuré a realizar un posible esquema; (i) responsables del tratamiento (participantes empoderados PF y PJ y mineros y nodos autónomos); (ii) encargados del tratamiento (nodos y mineros no autónomos, proveedores plataformas[1174], desarrolladores SC, BaaS); (iii) subencargado de tratamiento (desarrolladores y BaaS); (iv) titulares de datos interesados (participantes personas físicas no jurídicas).

12. Como hemos ido analizando, la pluralidad de sujetos en el ecosistema blockchain dificulta la asignación de responsabilidades en materia de protección de datos. En definitiva, habrá nodos que serán responsables y otros que serán encargados. El nivel de participación en el tratamiento de los datos será diferente en función del algoritmo de consenso y de la forma en que se haya configurado la tecnología. Por que cuando ellos sean autónomos; serán responsables, de lo contrario, serán encargados. Sin duda, se requerirá una *evaluación conjunta* preguntando sobre si los propósitos y *medios* (por ej. software instalado para el funcionamiento, red Hyperledger, Aeternity para SC, HLBox como plataforma) son determinados por más de una parte. La práctica muestra que no todos los responsables del ecosistema lo serán en la misma medida. La solución jurídica que se encuentra viene en el art. 26 RGPD (corresponsabilidad).

13. Así por ejemplo, un sistema blockchain de salud podría funcionar como un gestor de control de accesos y permisos para datos y registros de salud. En los modelos de ecosistemas Blockchain en salud - donde haya consorcios y múltiples partes- sería imprescindible el sistema SSI (o modelo de identidad digital soberana y "atómico"). Éste permitirá, entre otras cosas, empoderar al individuo/paciente/usuario mediante la *tokenización de los atributos* de la identidad digital a través las *credenciales,*

[1174] Las plataformas como *proveedores de servicios blockchain* también tendrán una posición jurídica que acometer. En China, por ejemplo, ya existe regulación para éstas y un registro público de las que han cumplido con la normativa (por ejemplo, *Alibaba Cloud Blockchain-as-a-Service BaaS* está incluida). En dicha normativa se les obliga a la estipulación de contratos de servicios con derechos y obligaciones de las partes. En cualquier caso, solo cuando los desarrolladores formen parte de la toma de decisiones se les podrá considerar responsables.

reclamaciones verificables o atestaciones a través de la web donde no existen terceros. En el *wallet* están contenidos los credenciales: quién o qué es el emisor del credencial y puede ser cualquier persona, organización o cosa a quién o qué fue emitido, por ejemplo un fabricante de dispositivo, un médico especializado, etc. También contendrá información sobre si ha sido modificado, por ejemplo, el médico certifica que los registros de salud del fabricante y la app de social diabetes son correctos, o si lo ha revocado por no estar de acuerdo, además de las preferencias, opiniones, consentimiento legal y declaraciones del individuo. Por ejemplo, Rosa es titular de datos y además de utilizar el DNI para muchas cosas tendrá un credencial como sujeto fuente de un ensayo clínico, otro como usaría de una app (por ejemplo, de *social diabetes)*, y otra como paciente de un consultorio médico local y otra como cliente de una aseguradora de salud (por ejemplo, *Adeslas)*. Así, por ejemplo, BENCHOUFI y RAVAUD (2017) ya explicaron las bondades de esta tecnología para mejorar la calidad de las investigaciones clínicas. GUY ZYSKIND, et al. ,(2015) ya trataron el uso de blockchain para proteger datos.

14. Hemos analizado que debido a la naturaleza de inmutabilidad de esta tecnología sería de difícil ejecución el cumplimiento de la RGPD.

14.1. No obstante, para el *derecho de rectificación*, se han presentado algunas posibles soluciones que se pueden acercar al cumplimiento normativo, aunque no libres de interrogantes y limitaciones. El recurso de los *enlaces o notificaciones suplementarias*) podría posibilitar que los titulares editaran (y agregar una modificación) a su información personal aunque no permitiría la modificación original y únicamente se podría hacer con los datos transaccionales y no con las claves públicas. Las *declaraciones - aclaraciones* al smart contract y la *edición por bifurcación ("forks")* pueden ser algunas soluciones. No obstante, ésta última resulta ser bastante costosa técnica y económicamente (tendrían que estar de acuerdo todos los nodos y habría que actualizar el software).

14.2. ¿En la medida es que resulte técnicamente imposible eliminar parte de las claves para el funcionamiento de la misma, se podría hablar de posibles exenciones a las obligaciones por motivos de limitaciones técnicas? Debe recordarse que el *derecho a ser olvidado no es un derecho absoluto* y los mayores problemas pueden surgir en los datos personales de las claves públicos y privadas. Desde mi punto de vista al igual que

piensa MILLARD (2018) de la Universidad Mary Queen, blockchain no será la última tecnología emergente en surgir (solo hay que pensar en la computación cuántica), por lo que no deberíamos de tener una posición conformista atascada en la justificación de las limitaciones tecnológicas. Tecnología es compatible con privacidad, estando atentos a las circunstancias y a cada caso.

14.3. Por ejemplo, la *poda de cadena de bloques* (PALM, 2017) podría acercarse a la solución de lo que se está buscando aunque sigue siendo controvertida. Lo mismo ocurre con el uso *de "hash de camaleón"* para volver a escribir el contenido de los bloques que tiene limitaciones (puede necesitar de un intermediario, no pueden eliminar las copias antiguas solo las recientes por lo que lo convierte en un proceso costoso. Desde mi punto de vista, las soluciones más acertadas se encontraban en torno a las *off-chain,* y *side-chain y middleware.* En cualquier caso, sería conveniente que el legislador o las Autoridades de Control (como AEPD) o el Comité Europeo de Protección de Datos se pronuncien al respecto. En Alemania por ejemplo, se acepta que los datos no se eliminen cuando el modo específico de almacenamiento lo hace imposible. Los problemas no son de carácter tecnológico sino más bien de cultura de privacidad de los participantes y un reto social de espíritu de comunidad y confianza desde los consorcios (también en salud). Las posibles soluciones que se presentarán en el futuro serán soluciones parciales para casos específicos, flexibles y diferentes a lo que venían conociendo los desarrolladores. Éstas serán disruptivas y sobre todo, creativas. Ya lo decía A. Einstein; "l*a imaginación es más importante que el conocimiento".*

15. Por último, he de señalar unas consideraciones a efectos prácticos. Por un lado, en los proyectos de blockchain (en whitepapers de proveedores, concretamente) se echa en falta el *enfoque jurídico del derecho fundamental de protección de datos de la privacidad*[1175] y mención expresa del RGPD (obligaciones y derechos de las partes)[1176]. Por otro lado, faltaría más participación de profesionales jurídicos (consultores[1177] y abogados expertos en privacidad y tecnología) que desarrollaran junto con los expertos técnicos los informes iniciales del proyecto. Por último, he de decir, que cada sector o industria es diferente y por tanto, los servicios tecnológicos y su impacto y alcance en los derechos y libertades resultan diferentes. La Industria de salud junto con el mercado

[1175]Vid. https://s3.ap-south-1.amazonaws.com/nhct.io/NHCT_Whitepaper.pdf
[1176] Vid. http://whitepaper.embleema.com/
[1177] Vid. https://www.grantthornton.es/globalassets/spain/folletos/rgpd-y-blockchain-final.pdf

tecnológico tiene sus particularidades específicas[1178]. En cualquier caso, como medidas específicas a tomar desde el momento inicial del sistema o proyectos, se recomienda a los desarrolladores que no almacenen los datos transaccionales dentro de una cadena de bloques y que se realicen EIPD respecto a las claves públicas. Además, se podría recomendar en el caso de blockchain privadas, los canales privados, hash, anonimización por capas o computación multipartita segura.

RESPECTO AL COMPLIANCE Y RESPONSABILIDAD EN MATERIA DE PROTECCIÓN DE DATOS PARA APLICAR A LA INDUSTRIA DEL CUIDADO DE LA SALUD DIGITAL.

Preguntas de investigación.
16. Tipos de riesgos posibles con repercusión legal nos encontraríamos en nuestro escenario. **17.** Analizar los instrumentos de derecho de protección de datos, al igual que la capacidad para representarse como medio de prueba y evidencia. **18.** Investigar cómo surge el "compliance en protección de datos" y qué es. **19.** Identificar situaciones críticas llamativas donde es clara la responsabilidad de determinados actores: Caso Boehringuer-Servicios Andaluz y Extremeño de Salud. **20.** Abordar las diferencias entre RSC y ética empresarial, si las hay. ¿De qué forma la tecnología podría ayudar en el ámbito de la responsabilidad y el cumplimiento normativo? ¿Qué tecnología emergente podría ser más conveniente? **21.** ¿Cómo es la institución de la indemnización en materia de protección de datos en el marco del régimen sancionador?

16. Serán ejemplos de riesgos una brecha de seguridad en el sistema de alojamiento cloud de un laboratorio privado o de cualquier hospital -donde los HCE han sido extraídos y vendidos en el mercado negro- o el hackeo de datos personales de salud extraídos de un dispositivo IoT de juguetes sexuales.

17. Está claro que la puesta en práctica de los *best practices corporativos* o la adhesión a códigos van a suponer, con el RGPD, un medio de prueba de responsabilidad proactiva ("accountability") y de cumplimiento normativo ("compliance") por parte de los clientes frente terceros (clientes, proveedores, competidores, autoridades de control, público) y que además servirán para el *"proceso de homologación"*[1179] de proveedores

[1178]Vid.https://www.healthcareitnews.com/news/how-blockchain-can-help-healthcares-patient-matching-problem

[1179]Ver https://blogs.itdmgroup.es/lorena-p-campillo/2017/01/cloud-computing-homologacion-de-proveedores-cloud-y-data-protection

tecnológicos[1180]. La dificultad de poner en marcha la máquina legisladora unida a la dificultad del legislador de entender la complejidad tecnológica hace conveniente la expansión del uso de la autorregulación en diferentes dimensiones y sectores. En mi opinión, el ecosistema de soft law y el sistema autorregulatorio permitirán evitar, anticipar, completar y estandarizar la legislación, compensando sus insuficiencias y limitaciones sobre todo en ámbitos tecnológicos. Todos ellos podrán coexistir en cierta armonía y complementariedad.

18. Como decíamos, el *compliance* no sólo surge a raíz de la reforma del código penal sino que tiene que ver con un resurgir de la cultura de cumplimiento global. Es más, no se limita a la responsabilidad penal de las PJ (quienes responden, directamente, por no ejercitar el debido control), sino que es una disciplina que reúne valores corporativos de las empresas y comportamientos correctos, también, en materia de protección de datos, privacidad y seguridad de la información sensible. Por tanto, en un código de cumplimiento normativo se debería incluir lo referente a protección de datos el cual debería ser conocido por todos los trabajadores (ej. Pensemos en una multinacional farmaceutica). Los proveedores tecnológicos son conscientes de la carga de responsabilidad que tendrán con sus clientes (hospitales, gobiernos, laboratorios, pacientes, usuarios, etc.) .Las funciones de los modelos de compliance serán entre otros el de la formación, capacitación y concienciación, la autoimposición normativa a través de códigos éticos[1181]o la creación de comités interdisciplinares formados por DPO, Compliance Officer, etc. Dicho lo anterior, ¿podría adoptar el *compliance corporate* una visión expansiva global, también como disciplina que reúne valores corporativos y comportamientos correctos y la visión de responsabilidad empresarial que la persona jurídica quiere asumir (PUYOL, 2017)[1182] , más específicamente en materia de protección de datos de las personas en pro de sus derechos y libertades que implicara a instituciones y organizaciones? A mi humilde modo de ver y tal como he explicado en el capítulo correspondiente, sí sería posible.

19. Situaciones críticas donde se produjeron extracciones ilegales de HCEs de pacientes como la del *Caso Boehringuer-Servicios Andaluz y Extremeño de Salud* me han hecho reflexionar y analizar los elementos desencadenantes, la efectividad de

[1180] Respecto a este punto, también hemos podido deducir que no todos los proveedores tecnológicos son iguales y tienen las mismas capacidades (o poder económico).
[1181] Vid. https://confilegal.com/20170118-puyo-javier-cumplimiento-normativo/
[1182] Idem.

respuestas por parte de las autoridades públicas y la repercusión negativa que ha podido tener en los derechos y libertades de las personas y en la sociedad en su conjunto. En sintonía con el escenario dinámico del que hemos hablado, aparecen los *canales de denuncia* como herramienta obligatoria (anteriormente era una recomendación) para la detección de ilícitos cometidos como el mencionado. Su uso se extenderá no sólo para trabajadores, sino para terceros, como por ejemplo, clientes o proveedores tecnológicos/subcontratistas.

20. La *RSC es* un área de práctica empresarial que aporta beneficios tangibles (reducción de costes, mejoras en la calidad, reducción de sanciones y costes en procedimientos judiciales o arbitrales) y beneficios intangibles (como la mejora de imagen reputacional). Hay que tener en cuenta las diferencias respecto a la ética empresarial. La *ética empresarial* suele ir ligada de códigos éticos de protección de datos, se refiere a comportamientos correctos y está condicionada por stakeholders y por su parte, la RSC se refiere al conjunto de actividades que la organización realiza para controlar el impacto de las tecnologías en las personas. Se me ocurre también, que la tecnología de blockchain/DLT posibilite en el futuro *smart contract* donde el titular de los datos sea resarcido de forma automática con la existencia de clausulas indemnizatorias ante posibles "*data breach*", combinándola con cloud computing (y la existencia de ciberseguros). En definitiva, ante escenarios dinámicos, soluciones dinámicas y flexibles. Además, si blockchain/DLT se ha implantado para otorgar trazabilidad en el contexto de compliance (control horario laboral, cumplimiento PRL[1183]); ¿por qué no podría servir para acreditar el cumplimiento en protección de datos (como hacen las empresas *Alisys o Asenfy)*? Desde mi humilde punto de vista, podríamos aprovecharnos de la tecnología para resolver problemas de la misma.

21. Con el RGPD, concretamente con el art. 83 se deberá "probar la existencia del daño aducido, y además, la relación de causalidad entre la acción u omisión del responsable con el daño producido. Por su parte, los art. 82.6 y 79 permiten al perjudicado por el tratamiento ilícito por optar por reclamar responsabilidad ante los órganos judiciales del Estado miembro donde el responsable o el encargado tenga su establecimiento, o bien donde el perjudicado tenga su domicilio (NIETO, 2016, 557-565). Ahora bien, ¿la responsabilidad civil derivada de la infracción en el ámbito del

[1183]Vid. https://www.beiota.com/

derecho administrativo supone desplazar al juez civil? Opino de la misma forma que HUERGO, quien señala que "es la imposición de una sanción la que permite que alguien (la Administración o los tribunales civiles, da igual) imponga también la responsabilidad civil, sin que puedan existir resoluciones "contradictorias". Si bien es cierto, la pericia del Juez es esencial, quizás, se podría realizar unos baremos prefijados por las autoridades (sobre todo pensando en indemnizaciones con cuantías bajas), evitando además con ello, el coste económico que supone al perjudicado acudir a sede judicial civil. En mi humilde opinión, la tendencia parece ir en la línea de este acercamiento competencial de la sede administrativa con la judicial, motivado principalmente por la sobrecarga de trabajo que posiblemente vayan recibiendo las autoridades de control a partir de ahora con la nueva norma en vigor. En cualquier caso, el legislador nacional, no se ha pronunciado por el momento, lo suficiente para aclarar y explicar el alcance de la institución de la indemnización.

RESPECTO AL DERECHO FUNDAMENTAL DE LA PROTECCIÓN DE DATOS PERSONALES. ENFOQUE DESDE EL ÁMBITO DE LA SALUD Y TECNOLOGÍA.

Preguntas de investigación
22. ¿El derecho a la protección de datos es un derecho humano? ¿ y fundamental? ¿y de la personalidad? **23.** ¿Se puede comerciar con los datos personales de salud? Sería conveniente extraer situaciones reales donde esto ocurre, por ejemplo, en aseguradoras o en tecnologías blockchain.

22. Ahora bien, hemos partido de la premisa de que el derecho a la protección de datos y la privacidad es un derecho humano (art. 12. Declaración Universal de los Derechos Humanos de 1948) y un derecho fundamental en virtud de nuestra constitución española (Art. 18.4 CE). Pero nuestro derecho también tiene encaje dentro del grupo de derechos de la personalidad que protege el ámbito moral de la persona.

23. Hemos analizado también que el derecho fundamental de protección de datos no se puede entregar, transferir o vender. Los derechos humanos son derechos intrínsecos y evidentes por sí mismos, al margen de que estén envueltos y protegidos por regulaciónn. No obstante, a mi modo de ver, se podría dejar abierta la posibilidad de que "algunos" datos personales pudieran existir en "alguna forma similar" de "quasipropiedad". Esta interpretación tiene que ser flexible y amplia. Por ejemplo, cabe preguntarnos; ¿podría ser lícito y legal *intercambiar "datos" por "medicamentos"* o

"datos" por "servicios de salud privados" como una teleconsulta, etc.? ; ¿ o "alquilar" información personal a cambio de una retribución, descuentos en pólizas de seguro o similar es cada vez más posible, sobre todo en contextos de sistemas *blockchain*/ DLT?. En la actualidad ya se está empoderando al individuo otorgándole herramientas para gestionar los datos y monetizar datos personales[1184].

RESPECTO A LAS CUESTIONES PREVIAS Y EL NUEVO RÉGIMEN JURÍDICO EN MATERIA DE PROTECCIÓN DE DATOS EN SALUD Y TECNOLOGÍA

Preguntas de investigación
24. ¿Dónde se concentran los datos de salud en España?, ¿el derecho de los ciudadanos a tener acceso a sus propios datos sanitarios es real? , ¿qué se podría hacer para conseguir su mayor efectividad? **25.** ¿Existen riesgos legales derivados de la reutilización de la información pública?, ¿podríamos considerar a los metadatos como datos personales?

24. En España, los datos de salud se concentran principalmente en las *Administraciones Públicas* como prestadores de asistencia sanitaria y cada vez se genera mayor información a través del Sector Privado con la industria farmacéutica y el sector tecnológico (ej. dispositivos móviles con apps de mHealth y wearables). El derecho de los ciudadanos a *tener acceso a sus propios datos sanitarios* es uno de los principios básicos del acervo de la Unión en materia de protección de datos y así se refleja en el Reglamento general de protección de datos. Aunque tal y como establece la Recomendación (UE) 2019/243, "la mayoría de los ciudadanos, sin embargo, aún no pueden acceder a sus datos sanitarios (ni compartirlos de forma segura) a través de las fronteras". El Consejo de la UE (2017) señalaba que "se necesitarían sistemas y herramientas flexibles que permitan a los ciudadanos *acceder* a sus propios datos, y a la *información* sobre el uso de sus datos, así como gestionar su *consentimiento* para el tratamiento y la comunicación de sus datos sanitarios, incluidos los destinados a un uso secundario".

[1184] El profesor RODOTÁ (2003) ya declaraba que nuestro cuerpo era una fuente abierta y continua para extraer datos. Esos datos a los que se refiere el profesor a las huellas dactilares, a la geometría de la mano o de los dedos o de las orejas, al iris, a la retina, a los rasgos, a los olores, a la voz, a la firma, a la utilización de un teclado, a la manera de andar, al ADN. Es decir, pasamos del control de nuestros datos personales convencionales (autodeterminación informativa) al control de nuestro cuerpo ("físico" y "electrónico"). En definitiva, como establecía, J.S.Mill., "e*l individuo es soberano sobre sí mismo, sobre su cuerpo y sobre su mente".*

25. Tras la investigación puedo decir que estoy de acuerdo con la autora ANDREU (2017) que viene a considerar que todavía no ha llegado el momento en que la información de open data sanitario se convierta en un valor añadido para el ciudadano.Los riesgos de privacidad que se pueden ocasionar en la *reutilización de la información pública* no pueden impedir que sea utilizada sino todo lo contrario, se debe impulsar tal y como se hace en la UE, pero siempre con implementación de garantías como la EIPD, auditorías periódicas, medidas coercitivas, penalizaciones, clausulas, etc.

Respecto a los *metadatos,* como he comentado, merecen especial atención ya que pueden ser considerados como datos personales, y así lo señala el TJUE. Se tratan de datos invisibles que pueden ser utilizados para fines publicitarios o de marketing de salud. Y es que puede sorprender pero a menudos se siguen clasificando como no sensibles" (PEREZ et al. 2018). Y es que la mayoría de los EEMM reconoce también la necesidad de que la protección de las comunicaciones constituya un derecho constitucional diferenciado (Comisión Europea, 2017). Veremos si existirán pronunciamientos expresos y necesarios por parte de los legisladores nacionales.

RESPECTO AL NUEVO RÉGIMEN JURÍDICO EN MATERIA DE PROTECCIÓN DE DATOS APLICADO A LA INDUSTRIA DEL CUIDADO DE LA SALUD DIGITAL

Preguntas de investigación.
26. ¿Hasta qué punto se podría haber aprovechado la denominada "información por capas" en beneficio del titular de datos antes de la aprobación de la LOPDGDD. (Pienso en legal design para la comunidad sordomuda en entornos de la Industria de la Salud Digital, por ejemplo). **27.** ¿De qué manera repercute la LOPDGDD en el ámbito de la investigación? ¿Se otorga mayores protecciones al titular fuente? , ¿Beneficia a la investigación en su conjunto? , ¿O exige más obligaciones a los investigadores? **28.** Según el RGPD, ¿cuándo los tratamientos automatizados serán legítimos?, ¿no hubiera sido conveniente que los EEMM regularan o desarrollaran el alcance de las decisiones automatizadas habida cuenta a tecnologías como el deep learning, por ejemplo, la intervención humana? **29.** ¿Las medidas técnicas y organizativas son obligaciones de medios o de resultados? **30.** Estudiar los retos que encuentran ante el Internet del ADN o con la llegada de la computación cuántica en medina respecto a la técnica de la anonimización. Sobre todo, pienso en la anonimización y su eficacia verdadera ante posibles reidentificaciones. **31.** Analizar la situación real de las aseguradoras interactivas como responsables del tratamiento de datos cuando se llevan a cabo decisiones automatizadas.

26. Uno de los aspectos que llamó mi atención en la nueva LOPDGDD tuvo que ver con la denominada «*información por capas*», donde el legislador nacional ha perdido la oportunidad de incoporar y tal y como han señalado estudiosos y colegas, soluciones que acercarían a la población al ámbito jurídico rígido y a veces opaco de las disposiciones, a través de la iconografía (o el diseño legal). De esta manera se podría hacer llegar de forma más clara, la información a los ciudadanos y usuarios, que necesitan conocer en escenarios de la complejidad de las tecnologías mencionadas en este trabajo por no mencionar colectivos como el de sordomudos.

27. Respecto a la *investigación científica,* como hemos visto, la AEPD señalaba en su informe que el RGPD no implicaba una alteración del marco normativo actualmente vigente en España, además se reconoce la importancia de la investigación biomédica y sus beneficios para los individuos y la sociedad en su conjunto. Esto va a permitir que la interpretación que se haga de las finalidades en la investigación biomédica pueda ser más amplia". Y es que la LOPDGDD amplía las finalidades para las que se puede otorgar el consentimiento al tratamiento; recoge la posibilidad de reutilizar la información sobre la que se ya se haya prestado consentimiento con anterioridad; recoge el uso de datos pseudonimizados como una opción para facilitar la investigación sanitaria incluyendo garantías para evitar la reidentificación de los afectados; y regula las garantías de este tratamiento, incluyendo la intervención de los Comités de Ética de la Investigación o, en su defecto, del DPO o de un experto en protección de datos personales. El legislador refuerza el derecho a la protección de datos del titular de datos personales en el contexto de la investigación exigiendo a los investigadores la realización de una EIPD donde se incluye detalle y análisis del riesgo de la *"reidentificación"* de los datos anonimizados o pseudonimizados, y las medidas correspondientes. Así por ejemplo, el profesor MARTÍNEZ MARTÍNEZ (2017,260) aconseja que investigadores o responsables del tratamiento opten como base legitimadora el consentimiento del paciente puesto que implicaría la interpretación estricta parcelando un área concreta de investigación.

28. Los tratamientos automatizados tendrán legitimación siempre que exista; el consentimiento expreso o por motivos de interés público; el derecho a obtener una intervención humana; el derecho a impugnar la decisión. Ahora bien, me pregunté al inicio de esta investigación, ¿no será el momento oportuno para aprovechar y regular de alguna manera el alcance de los EEMM en estas decisiones automatizadas teniendo en cuenta el rápido avance tecnológico de tecnologías como *deep learning* en salud? ¿Por

qué no regular aspectos de la intervención humana, o la explicación o justificación que debe otorgarse al interesado y así conseguir más seguridad jurídica? A mi humilde modo de ver y en cualquier caso, se debería es necesario optar por llevar a cabo todas las máximas coberturas para asegurar la protección a los derechos y libertades de las personas. Se requiere de mayor protección y seguridad jurídica a los titulares de datos. Respecto al "derecho de explicación" MALGIERI (2018), se pregunta si los legisladores nacionales podrán ampliar este alcance o si estarán permitidas las "decisiones positivas" o qué garantías podrán proteger mejor al individuo. Este autor llama la atención las iniciativas de EEMM como: Francia y Hungría que garantizan el *derecho a la legibilidad / explicación* de las decisiones algorítmicas o Irlanda y Reino Unido *regulan la intervención humana* en la decisión algorítmica a través de un mecanismo efectivo de rendición de cuentas (por ejemplo, notificación, explicación de por qué no se ha aceptado tal impugnación, etc.). El debate estará abierto durante un tiempo.

29. Por otro lado, he de subrayar otra cuestión. Cuando se hablan de *medidas obligatorias,* éstas deben obtener un resultado (la no vulneración de los derechos de las personas), es decir, no se tratará de una obligación de medios.

30. Pero, ¿qué retos se nos presentan respecto a la técnica de la anonimización? La Guía de la AEPD sobre "Orientaciones y garantías en los procedimientos de anonimización de datos personales" no permite albergar grandes esperanzas sobre esta técnica declarando que no es posible garantizar el 100% de la *no* reidentificación de las personas, por lo que será necesario sustentar la fortaleza de la anonimización en medidas de evaluación de impacto (EIPD), organizativas, de seguridad de la información, tecnológicas y, en definitiva, cualquier medida que sirva tanto para atenuar los riesgos de reidentificación de las personas como para paliar las consecuencias de que éstos se materialicen". En todo caso, la AEPD aconseja entre otras medidas, técnicas que requieran un coste lo suficientemente alto que la "reidentificación" resulte ser inviable o inasumible en términos de "esfuerzo-beneficio". El rápido avance tecnológico podría dejar obsoletas las técnicas de anonimización. Por ejemplo, pensemos en los perfiles genéticos donde si se utiliza únicamente la técnica de

eliminación de la identidad del donante. Según autores[1185], se ha demostrado que al combinar los recursos genéticos disponibles para el público (p. ej., resultados de consultas en motores de búsqueda) y los metadatos sobre donantes de ADN (fecha de donación, edad o lugar de residencia) se puede revelar la identidad de determinadas personas aunque el ADN se haya donado de forma anónima.

31. Respecto al marco normativo de las *aseguradoras digitales,* a mi modo de ver, sería necesario ampliar el alcance del deber de información de las aseguradoras lo máximo posible en situaciones donde los *dispositivos wearables* (con naturaleza similar a los "cuestionarios clásicos") toman decisiones automatizadas determinantes para los derechos y libertades de las personas.

RESPECTO A LAS IMPLICACIONES ÉTICAS DESDE EL PUNTO DE VISTA DE LA PROTECCIÓN DE DATOS Y LA PRIVACIDAD EN LA INDUSTRIA DEL CUIDADO DE LA SALUD DIGITAL

Preguntas de investigación.

32. Analizar los problemas éticos que podrían surgir desde la perspectiva de la investigación científica como bien común. Por ejemplo, pienso en posibles intereses ocultos. **33.** ¿Están seguros los ciudadanos, usuarios o titulares de datos con las AAPP de salud? ¿cómo se podría minimizar los riesgos o posibles vulnerabilidades en los derechos y libertades de las personas? **34.** ¿Qué es la ética de los datos? ¿De qué forma podría la ética de los datos solucionar los desafíos que se presentan con la transformación digital de la Industria? **35.** ¿Se va a llevar la ética a las empresas (responsables y encargados de tratamiento) de forma similiar a lo que se conoce como RSE empresarial? **36.** ¿Cómo será la ética del futuro que podremos aplicar a nuestro objeto de estudio?

32. Desde una perspectiva de la *investigación científica como bien común* nos surgían interrogantes como; ¿de qué manera sabemos que no hay intereses ocultos ni favoritismos entre empresas de la industria y la promoción de fármacos? ¿podrían los titulares de datos personales tener beneficio económico o compensación de algún tipo? Todos esto nos lleva a plantearnos que la sociedad está preocupada y como señala *Locke*; *"lo que te preocupa, te controla"*.

[1185] Álvarez Hazas, G.Anonimización de datos personales de la investigación. Perspectiva jurídica y práctica. Mallorca, 2018. Recuperado de https://gahazas.files.wordpress.com/2018/11/anonimizacic3b3n-de-datos-personales-para-investigacic3b3n_v3.pdf

33. A pesar de que las encuestas señalen que los ciudadanos tienen seguridad en las AAPP sanitarias, no hay mucha concienciación del carácter de categoría especial que suponen los datos contenidos en los HCE. El impacto negativo de Big Data e IA sobre los derechos y libertades de las personas, posiblemente, se podrían superar gracias a la ética de datos y a medidas técnicas y organizativas basadas en la responsabilidad proactiva -de los participantes implicados en el ecosistema creado-, a la privacidad desde el diseño, y a una anonimización irreversible y a un buen gobierno de datos.

34. Según TRANBERG y HASSELBACH (2019, 58) "no podemos entender la privacidad como una *cuestión de confianza,* sólo como una cuestión de protección, cumplimiento y carga administrativa. La forma en que abordamos y manejamos los datos personales y la privacidad es un indicador básico de confianza". Cuando hablábamos de *ética de los datos* (FLORIDI y TADEO, 2016) nos referíamos a la ética vinculada a los principios y valores en los que se basan las leyes de protección de datos personales y derechos humanos que podrán dar solución a los desafíos que hemos ido citando. Algunos de ellos, tienen que ver con *"black box"* como las cajas negras y podrán ser mitigados, en todo caso, a través de medidas contempladas por ejemplo, en las directrices de ética para IA confiable, en las recomendaciones de la CNIL o por medio de elaboración de guías algorítmicas o soluciones desde los valores. El uso de la tecnología genera datos vaporosos con todas sus limitaciones, sesgos y manipulaciones (COTINO, 2017).

35. Aunque ya lo hemos mencionado a lo largo del trabajo, nos encontramos con una oportunidad para llevar la ética a las organizaciones en forma, también, de RSE como contribución activa y voluntaria al mejoramiento social que tiene por objetivo mejorar la situación competitiva y valorativa de la empresa teniendo en cuenta el respeto del derecho fundamental de la protección de datos de las personas.

36. La ética del futuro pasará a ser de "reglas" para convertirse en "valores". *"La ética puede ser la obra de arte más grande de la humanidad"* (BUTARELLI, 2018). El propio SEDP, ha señalado que en la actual Era Digital, el cumplimiento de la ley no es suficiente, tenemos que considerar la *dimensión ética* del procesamiento de datos . Ahora bien, ¿podrá articularse adecuadamente la ética conjuntamente con el Derecho para dar solución a los riesgos de los que estamos hablando).

FUTURAS LÍNEAS DE INVESTIGACIÓN.

Preguntas de investigación
1. Decisiones automatizadas, aseguradoras virtuales y árboles de decisión.
2. Tecnologías cuánticas aplicadas a la Medicina.
3. La "privacidad mental" y deep learning

1. En lo referente a las *decisiones automatizadas de datos personales* (p.e. en seguros de salud interactivos). Pongamos un ejemplo; el sistema de IA rechaza la solicitud de un individuo ya que no cumple ciertos parámetros (por ejemplo, no alcanza cierto número de pasos al día según el dispositivo *wearable fitbit*) a través de decisiones automatizadas.

¿Hasta qué punto éstas tendrán que justificarse? ¿Deberán explicar los "árboles de decisión" que posibiliten la ruta de aprendizaje? ¿Qué alcance tomará esa explicación? ¿El derecho a la oposición y a la intervención humana es suficiente para garantizar el respeto a los derechos y libertades de las personas? ¿Las aseguradoras podrán solucionar -como responsables del tratamiento *en el marco de* los *proyectos de big data de salud*- según el RGPD, *desafíos tales* como la discriminación, la falta de transparencia, los conflictos por finalidades incompatibles, la errónea legitimación o la reversibilidad de la anonimización? ¿De qué manera? ¿Sería necesario un desarrollo normativo por parte del legislador nacional respecto a lo mencionado?

2. Respecto a las tecnologías cuánticas aplicadas a la medicina[1186].

Con la llegada de éstas, se podrá permitir el desarrollo de medicamentos a medida, por ejemplo. La cuántica permite realizar varios cálculos o simulaciones de manera simultánea en lugar de secuencial, permitiendo diseñar nuevos medicamentos con los computadores de manera mucho más rápida y barata. Ahora bien, ¿somos conscientes de las repercusiones que en materia de protección de datos va a tener? ¿Cuáles serán? ¿La encriptación cuántica otorgará suficientes soluciones para "salvar" a la privacidad y la protección de datos tras las vulnerabilidades que surgirán en

[1186]Vid https://blogs.iadb.org/salud/es/tecnologias-cuanticas/?fbclid=IwAR3qOOmjmw7OSqTrpipx353wB97jgWdbbYjN2uB3eWv_m3_yVEmac59X56A

ciberseguridad? ¿La *ética cuántica* podrá ser una posible solución para perfilar un marco ético-jurídico de responsabilidades? Desde mi humilde opinión, vaticino un amplio campo de investigación donde académicos, profesionales y stakeholders deberán trabajar para diseñar un marco ético-legal que impida la posición más perversa de la computación cuántica como arma de guerra contra la ciberseguridad. Aquellos países -aliados con los mejores gigantes tecnológicos- que puedan desarrollar antes esta tecnología, tendrán el poder del mundo en sus manos. Los desarrollos tecnológicos amenazan los ataques cibernéticos mejorados, la vigilancia más amplia y la seguridad nacional desestabilizada (JOHNSON, 2019). En cualquier caso, si la ciberseguridad "desaparece", ¿dónde quedará el derecho fundamental de la protección de datos y la privacidad de las personas?

3. La "privacidad mental" y deep learning**.**

Por otro lado, poniendo nuestro punto de mira en el futuro, hemos comprobado que ya hay investigadores japoneses que están diseñando una red neuronal (*"deep learning*") para que smartphones puedan leer mentes mediante el escaneo de las ondas cerebrales dentro de cinco años (LIN et al, 2018). Entonces, ante escenarios como éste o el de la computación cuántica, podremos lanzar *preguntas de investigación futuras* como ¿dónde quedará el derecho fundamental de la protección de datos y la privacidad de las personas? ¿Qué información debe liberarse a la red pública sobre los pacientes? ¿qué consecuencias podría tener que los cerebros pudieran estar conectados entre sí para la "*privacidad mental*"o que se pudiera acceder a la información -y apropiarse de ella- de un cerebro manipular o insertar información?¿la ley podrá ir sola en este camino o necesitará de la ética?

BIBLIOGRAFIA

1. ABERASTURI GORRIÑO, Unai "El derecho a la indemnización el art.19 de la LOPD" P.176. Recuperado de http://w.aragon.es/estaticos/GobiernoAragon/Organismos/InstitutoAragonesAdministracionPublica/Areas/03_Revista_Aragonesa_Formacion/04%20Unai%20Aberasturi.pdf
2. ACQUISTI, A. Leslie John, George Loewenstein (2013). What is privacy worth?, The Journal of Legal Studies, Vol. 42, No. 2, *The University Chicago Press*, https://www.cmu.edu/dietrich/sds/docs/loewenstein/WhatPrivacyWorth.pdf
3. ADAMS ELBRIDGE, L., "The Right to Privacy and its Relation to the Law of Libel", 39 American Law Review, 37, Enero-Febrero 1905, pp 37–58.
4. ALCACER GUIRAO,R., "Cumplimiento penal por la persona jurídica y derechos fundamentales: la intimidad como límite a la vigilancia empresarial", *Diario La Ley* , Núm. 8053, Sección Doctrina, 2 Abr. 2013, Año XXXIV, Ref.D-118, LA LEY 1685/2013 . En AGUSTINA, J.R. "el DPO en el marco de la responsabilidad penal". Recuperado de https://www.academia.edu/11420153/El_Data_Protection_Officer_en_el_marco_de_la_responsabilidad_penal_de_las_personas_jur%C3%ADdicas_Consideraciones_a_la_luz_del_nuevo_Reglamento_Europeo_en_materia_de_protecci%C3%B3n_de_datos
5. ANDREU MARTÍNEZ, M.B. (2017) Open Data En El Ámbito Sanitario Y Su Compatibilidad Con La Privacidad Del Paciente. Les Éditions del'IMODEV (Improving Public Policies in a Digital World). Open Journals. *Revue Internationale des Gouvernements Ouverts*. Vol. 5. Recuperado de http://ojs.imodev.org/index.php/RIGO/article/view/200/330
6. ALLENDE LÓPEZ, M. Blockchain: cómo desarrollar confianza en entornos complejos para generar valor de impacto social. *Banco Interamericano de Desarrollo*. Recuperado de https://webimages.iadb.org/publications/spanish/document/Blockchain-C%C3%B3mo-desarrollar-confianza-en-entornos-complejos-para-generar-valor-de-impacto-social.pdf
7. ALVAREZ GONZALEZ, S. La utilización de datos genéticos por las compañías aseguradoras. Instituto de Ciencias del Seguro. *Fundación Mapfre*. 2006. Pag 27. Recuperado de http://fundacionmapfre.com/ccm/content/documentos/fundacion/cs-seguro/libros/la-utilizacion-de-datos-geneticos-por-las-companias-aseguradoras-106.pdf
8. Alavarez Rigaudias, C. (2016) . Tratamiento de datos de salud. En *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad.* Págs. 171-185. Dtor. J.L. Piñar. Madrid: Editorial Reus.
9. ARROYO MARTÍNEZ, I. (2003). Ley de Contrato de Seguro, p. 35. Madrid : Tecnos
10. ATENIESE G. et al. (2017). Redactable Blockchain - or - Rewriting History in Bitcoin and Friends. *IEEE European Symposium.* Recuperado de http://ieeexplore.ieee.org/document/7961975/
11. AUFFERMANN WF, Chetlen AL, Colucci AT, DeQuesada Ii IM, Grajo JR, Heller MT et al. (2015), Online Social Networking for Radiology. *Academic Radiology* ;22(1):3-13.
12. BAMBERFER, K., Mulligan, D. (1 de enero de 2010). Privacy on the books and on the ground. *Berkeley Law Scholarship Repository*. Recuperado de https://www.technologyreview.es/s/10266/no-podemos-permitirnos-usar-inadecuadamente-los-datos-del-paciente

13. BARRY, V. E., (1979) *Moral Issues in Business*, Belmont, CA. En CONVERSO, Domenico, The accountability of data controllers in relation to cloud providers, 2013. Recuperado de http://arno.uvt.nl/show.cgi?fid=131417
14. BELL, A., Chetty R.,Jaravel X. & Petkova N& Van Reenen, J. 2019. "Who Becomes an Inventor in America? The Importance of Exposure to Innovation*," The Quarterly Journal of Economics, vol 134(2), pages 647-713. Recuperado de https://www.nber.org/papers/w24062
15. BERBERICH, M., Steiner, M., (2017) "Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?", 2 Eur. Data Prot. L. Rev., 422.
16. BENCHOUFI, M, RAVAUD P. (19 de julio de 2017). Blockchain technology for improving clinical research quality. *BMC Trialsjournal*. Recuperado de https://trialsjournal.biomedcentral.com/articles/10.1186/s13063-017-2035-z
17. BENNET, B., (2010) *International privacy standards: can accountability ever be adequate?,* Privacy Laws & Business International Newletter, p. 21. En CONVERSO, D., The accountability of data controllers in relation to cloud providers, 2013.
18. BERLINSKI, D. (2005). Infinite Ascent: A Short History of Mathematics. *New york: Modern Library*, p. 45.
19. BLANCO PÉREZ-RUBIO, L. (2014). Obligaciones de medios y obligaciones de resultado: ¿tiene relevancia jurídica su distinción? *Universidad Carlos III.* Recuperado de https://e-revistas.uc3m.es/index.php/CDT/article/viewFile/2260/1199
20. CARNICERO, J. SEIS, Sociedad Española de Informática de la Salud (18 de diciembre de 2003). De la historia clínica a la historia de salud electrónica. *Informes SEIS*. Coord. Recuperado en https://docplayer.es/3607660-Informes-seis-de-la-historia-clinica-a-la-historia-de-salud-electronica-pamplona-18-de-diciembre-de-2003.html Pág. 24-5
21. CARRETERO, P.; de la Peña , P; Moreno Fdz., Aitor; (2018) . Blockchain en Sanidad. *Revista de la Sociedad Española de Informática y Salud.* Blockchain en salud. ¿Realidad o quimera?. Núm., 128. PP. 15-7. Recuperado de https://seis.es/wp-content/uploads/2018/04/128.pdf pp17
22. CASADO, M, do Céu Patrão Neves, M. Itziar de Lecuona, Carvalho, A.S., Araújo J. (2016) . Declaración sobre integridad científica en investigación e innovación responsable. Cátedra Unesco de Bioética de la Universidad de Barcelona. Recuperado de http://www.publicacions.ub.edu/refs/observatoriBioEticaDret/documents/08489.pdf
23. CATE ,F; CULLEN, P. MAYER-SCHÖNBERGER, V. (2014). Principios de protección de datos para el S. XXI. Revisión de las directrices de 1980 de la OCDE. *Universidad Oxford.* Recuperado de https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf
24. CASTELLANO ARROYO, M. (1944). El consentimiento informado de los pacientes. *Manual de bioética general.* Ed. Dr. Aquilino Polaino-Lorente. Madrid.
25. CLAERHOUT, B., & DeMoor, G. J. E. (2005). Privacy protection for clinical and genomic data: The use of privacyenhancing techniques in medicine. *International Journal of Medical Informatics*, 74(2–4), 257–265. Recuperado de http://doi.org/10.1016/j.ijmedinf.2004.03.008
26. CLIMACO VALIENTE, Ernesto (2012) Tesina "Géneis histórica-normativa del derecho a la protección de los datos personales desde el derecho comparado a propósito de su fundamento" (Pag. 17)
27. CHABERT, J.L. ed. Al., (1999) *.A History of Algorithms: From the Pebble to the Microchip*, traducido por Chris Weeks. en Steiner, C.. . *Una breve historia de hombres y*

algoritmos. Recuperado de https://catedradatos.com.ar/media/5.-Steiner-Una-breve-historia-de.pdf traducido por Álamo, Alonso y Ortiz.

28. COLMENAREJO FERNÁNDEZ, R. (2017). Una ética para Big Data. Introducción a la gestión ética de datos masivos. *Editorial UOC*.
29. COMOCK, M., (2013). *Legal definitions of responsibility, accountability and liability,* Nursing children and young people, Aprile 2011. En CONVERSO, D., The accountability of data controllers in relation to cloud providers.
30. CORTEZ, N. (2014). The Mobile Health Revolution? *Law Review University of California Davis*. pp. 1173. Recuperado de https://lawreview.law.ucdavis.edu/issues/47/4/Articles/47-4_Cortez.pdf
31. COTINO HUESO, L. (2017) . Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales. *Universidad de Valencia*. Nº 24, págs. 131-15
32. COTINO HUESO, L.(2017). Ética de datos, sociedad y ciudadanía. *Dilemata,* año 9, nº 24, 132. https://www.dilemata.net/revista/index.php/dilemata/article/view/412000116/506DONOTI, Pierpaolo (1994). Manual de Sociología de la Salud. Ediciones Díaz de Santo, SA. Pp. 30. España.
33. CULLEN, P.; GLASGOW, J., STAN, C. (Octubre 2015) Introduction to the HGP framework. Information Accountability Foundation, pp. 29. Recuperado de http://informationaccountability.org/wp-content/uploads/HGP-Overview.pdf y http://informationaccountability.org/effective-data-protection-governance-project/
34. D'ASARO Biondo Information Technology (2017) From Automated work to virtual wars: The future by those who are shaping it. Portfolio Penguin House, Londres, 290 en Ibáñez, J. W. (2018). *Blockchain: Primeras cuestiones en el ordenamiento español.* Editorial Dykinson
35. D'ACQUISTO, G., et al.. (2015). Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics. *Cornell University.* Recuperado de https://arxiv.org/abs/1512.06000
36. DE BRONKART, D. (02 ABril 2013). How the e-patient community helped save my life: an essay by *BMJ* 2013; 346 doi: Recuperado de https://doi.org/10.1136/bmj.f1990
37. DEBIÉS, E. (2017). Apertura de datos de salud en Francia, impacto en la investigación y la Seguridad Social. *Revistas UM Bioderecho*. Núm. 5, pág. 7. Recuperado de https://digitum.um.es/xmlui/bitstream/10201/54099/1/Apertura%20de%20datos%20de%20salud%20en%20Francia%2C%20impacto%20en%20la%20investigacion%20y%20la%20seguridad%20social.pdfELISH, M.C. (2016). Moral Crumple Zones: Cautionary Tales in Human-Robot Interation. En We Robot Conference Paper Draft. Recuperado de http://robots.law.miami.edu/2016/wp-content/uploads/2015/07/Elish_cautionary-tales_prelim_draft.pdf
38. EYSENBACH G. (2001). What is e-health? J Med Internet Res. Apr-Jun;3(2):E20. PubMed PMID: 11720962; PubMed Central PMCID: PMC1761894. Recuperado en http://www.jmir.org/2001/2/e20/
39. FERNÁNDEZ CONTE, LEÓN BURGOS (2016). Antecedentes y proceso de reforma sobre protección de datos en la Unión Europea. En *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad.* Págs. 35-50. Dtor. Piñar Mañas. Madrid: Editorial Reus.

40. FINK, M. (2018). Blockchains y Protección de datos en la Unión Europea. *Der Juristiche Verlag Lexxion.* Vol. 4, No. 1. Pp. 17-35. Recuperado de https://edpl.lexxion.eu/article/edpl/2018/1/6/display/html
41. FICK, Michèle, Blockchains and Data Protection in the European Union (November 30, 2017). Max Planck Institute for Innovation & Competition Research Paper No. 18-01. Available at SSRN: https://ssrn.com/abstract=3080322FOX S. (2008). The Engaged E-patient Population. Pew Internet Am Life 1-4. or http://dx.doi.org/10.2139/ssrn.3080322
42. FERNÁNDEZ HIERRO. J.L. (2002). *Régimen jurídico general de la historia clínica*. En la obra coordinada *La Historia Clínica* por él mismo, pp. 172-6.Edit. Comares, Granada.
43. FLORIDI, L., TADDEO, M. (2016). What is data ethics? Phil. Trans. R. Soc. A 374: 20160360. Recuperado de http://dx.doi.org/10.1098/rsta.2016.0360
44. FOZ X., Martinero, J., Morales, JR, Carrascosa, C. (2017) *Blockchain: La revolución industrial de internet*. En *Aspectos legales de los ICO, Smart Contracts y DAO* (pp 176). Barcelona: Editorial Gestion2000.
45. FRANCO DE FRANCO, M.J.; Perdomo, Y. C; Godoy, E. (2010) Preeminencia de la Ética sobre la Tecnología *Revista Daena . Revista Internacional de Buena Conciencia.* vol. 5 Número 1, p81-97. 17p.Recuperado de http://www.spentamexico.org/v5-n1/5(1)81-97.pdf
46. GAMBA, J., RASHED, M., RAZAGHPANAH, A., TAPIADOR J. ,VALLINA-RODRÍGUEZ, N. An Analysis of Pre-installed Android Software. Recuperado de https://haystack.mobi/papers/preinstalledAndroidSW_preprint.pdf
47. GAYO, M. (9 de enero de 2019). La inteligencia artificial ayuda a identificar síndormes genéticos raros. *ABC Enfermedades*. Recuperado de https://www.abc.es/salud/enfermedades/abci-inteligencia-artificial-ayuda-identificar-sindromes-geneticos-raros-201901071700_noticia.html
48. GARRIGA DOMÍNGUEZ, Ana, *"Tratamiento de Datos Personales y Derechos Fundamentales"*, Editorial Dykinson, Madrid, 2004, página 19GIANNOPOULOU, A.; Ferrari, V. (2018) . Distributed Data Protection And Liability On Blockchains. *INTERNET SCIENCE. 5th International Conference, INSCI 2018*. St.Petersburg, Russia, October 24-26, Proceedings, Vol. 2. Workshops Recuperado de https://pure.uva.nl/ws/files/31868271/SSRN_id3316954.pdf Pág. 9.
49. GARCÍA GONZÁLEZ, A. La Dignidad Humana: Núcleo Duro de los Derechos Humanos**.** *Universidad Latina de América.* Recuperado de http://www.unla.mx/iusunla28/reflexion/La%20Dignidad%20Humana.htm
50. GÓMEZ PINZÓN, J.C. (2017). *Implementación de proyectos de Big Data*. (Informe final monográfico, Universidad Libre de Colombia). Págs. 8-11.Recuperado de https://repository.unilibre.edu.co/bitstream/handle/10901/11214/Implementacion%20de%20proyectosde%20Big%20Data.pdf?sequence=1&isAllowed=y
51. GÓMEZ –ULLARTE RASINES, Susana (2014). Historia de los derechos de los pacientes. *Revista de Derecho UNED*, núm. 15.
52. GONZÁLEZ, P.A. (2017). Responsabilidad proactiva en los tratamientos masivos de datos. DILEMATA. Año 9, Num. 24, pp. 115-129. Recuperado de https://www.dilemata.net/revista/index.php/dilemata/article/view/412000103/493
53. GUY ZYSKIND, et al., Descentralización de la privacidad: uso de Blockchain para proteger datos personales, *2015 IEEE Sec. talleres de privacidad* 180, 181 (2015).
54. HAILAY D, ROOINE R. (2002) Systematic review of evidence for the benefits of telemedicine. *J Telemed Telecare* ;8:1-77
55. HARARI, Yuval Noah (2017). *Homo Deus: A Brief History of Tomorrow*. UK: Vintage, Penguin Random House. p. 440.

56. HARTZOG, W., Stutzman, F.D.. (2013) . Obscurity by Design, *Washington Law Review*, Vol. 88, 386. Recuperado de https://ssrn.com/abstract=2284583.
57. HERRERA RUÍZ, F.J. (2010). *Selección de riesgo en el Seguro de Salud. Seguros de Asistencia Sanitaria.* (Trabajo fin de Máster, Universidad de Barcelona). Recuperado de http://www.servidor-gestisqs.com/ub/intranet/pdf/tesis_alumnos/Javier_Herrera.Seleccion_Salud.pdf
58. HOOD, L. (2013). Systems Biology and P4 Medicine: Past, Present, and Future. Rambam Maimonides Med J
59. HIL R. (2016). "What an algorithm is?" *Philosophy and Technology* 29 Nº 1 pp. 35-59 en; Monasterio, A. Ética algorítmica: Implicaciones éticas de una sociedad cada vez más gobernada por algoritmos, 2017.
60. HISSEMBAUM, H., Patterson, H. Biosensing in Context: Health Privacy in a Connect World. Recuperado de https://nissenbaum.tech.cornell.edu/papers/Nissenbaum%20H%20Patterson%20H_Biosensing%20in%20Context.pdf
61. HUERGO LORA, A. Sanciones administrativas y responsabilidad civil.(2015). Recuperado de https://almacendederecho.org/sanciones-administrativas-y-responsabilidad-civil/
62. IBAÑEZ, J. W. (2018). *Blockchain: Primeras cuestiones en el ordenamiento español.* Editorial DYKINSON
63. JIMÉNEZ, J. (2016). Ya no se puede practica bien la medicina sin una inteligencia artificial al lado. *Xataca*. Recuperado de https://www.xataka.com/medicina-y-salud/ha-llegado-el-momento-en-que-no-podremos-practicar-la-medicina-sin-una-inteligencia-artificial-al-lado
64. Johnson, Walter G., Governance Tools for the Second Quantum Revolution (February 28, 2019). Jurimetrics, 2019, Forthcoming. Disponible en SSRN: https://ssrn.com/abstract=3350830
65. JOLLEY, N. ed.al, The Cambridge Companion to Leibniz. *Cambridge University Press*, 1995, p. 251. ; en Steiner, C.; Una breve historia de hombres y algoritmos
66. LABRIQUE, A B., et al. (2013). Issues in mHealth research involving persons living with HIV/AIDS and substance abuse. AIDS research and treatment", 1-6. US National Library of Medicine. *AIDS Res Treah.* Recuperado de https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3792525/
67. LÁZARO J., GRACIA, D. (2006). La relación médico-enfermo a través de la historia. *Anales del Sistema Sanitario de Navarra*. Vol. 29, supl.3. Pamplona. Recuperado en http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1137-66272006000600002
68. LEE, Y. et. Al. (2018). PRETZEL: Opening the Black Box of Machine Learning Prediction Serving Systems. *aeXiv of Cornell University*. Recuperado de https://arxiv.org/abs/1810.06115
69. LEENEN, PINET y PRIMS (1986). Trends in Health *legislation in Europe*. Masson.
70. LIKAMWA R.et al., (2011). MoodScope: Building a Mood Sensor from Smartphone Usage Patterns. Recuperado de http://www.ruf.rice.edu/~mobile/publications/likamwa2013mobisys2.pdf.
71. LIKAMWA R. et al. "Can your smartphone infer your mood?" .Recuperado en http://www.ruf.rice.edu/~mobile/publications/likamwa11phonesense.pdf
72. LIN, F. et al. (2018). Brain Password: A Secure and Truly Cancelable Brain Biometrics for Smart Headwear. *MobiSys '18*, June 10–15, Munich, Germany. Recuperado de http://cse.ucdenver.edu/~linfen/papers/2018_Mobisys_Brain_Password.pdf

73. LIU, Y, Niu, J., Yang, L., Shu, L. (2014). eBPlatform: An IoT-bases system for NCD patients homecare in China. En *IEEE Global Communications Conference.* Recuperado de http://ieeexplore.ieee.org/document/7037175/?reload=true
74. LOBER WB, Flowers JL. (2011), Consumer Empowerment in Health Care Amid the Internet and Social Media. *Seminars in Oncology Nursing* ;27(3):169-82.
75. LOTANERO, M. Governing Artificial Intelligence: Upholding human rights & dignity. *Data & Society.* Recuperado de https://datasociety.net/wp-content/uploads/2018/10/DataSociety_Governing_Artificial_Intelligence_Upholding_Human_Rights.pdf
76. LOZOYA DE DIEGO, A.,Villalba de Benito, M.T., Arias Pau, M. (2017). Taxonomía de información personal de salud para garantizar la privacidad de los individuos". El profesional de la información. marzo-abril, V.26, N.2. Recuperado de http://www.elprofesionaldelainformacion.com/contenidos/2017/mar/16.pdf
77. LOWE MM, Blaser DA, Cono L, Arcona S, Ko J, Sasane R, Mechas P (2016). "Aumento de la participación del paciente en el desarrollo de fármacos". Valor en salud . 19 (6): 869–878. doi : 10.1016 / j.jval.2016.04.009 . PMID 27712716 .
78. MALIN, B., KARP, D., & SCHEUERNANN, R. H. (2010). Technical and Policy Approaches to Balancing Patient Privacy and Data Sharing in Clinical and Translational Research. *Journal of Investigative Medicine* : The Official Publication of the American Federation for Clinical Research, 58(1), 11–18. Recuperado de http://doi.org/10.231/JIM.0b013e3181c9b2ea
79. MALGIERI, Gianclaudio. Automated Decision-Making in the EU Member States Laws: The Right to Explanation and Other 'Suitable Safeguards' (August 17, 2018). Recuperado de https://ssrn.com/abstract=3233611 o http://dx.doi.org/10.2139/ssrn.3233611
80. MARTÍN MIRALLES, R. (dic. 2010). Cloud computing y protección de datos. En VI Congreso Internet, Derecho y Política. Cloud computing: El derecho y la política suben a la nube". (Monográfico en línea). *IDP. Revista de los Estudios de Derecho y Ciencia Política.* N.11. UOC. Recuperado de http://idp.uoc.edu/ojs/index.php/idp/article/view/n11-miralles/n11-miralles-esp%3E ISSN 1699-8154.
81. MARTÍN MIRALLES, R. (2013). Big Data vs Small low. *Congrés IDP 2013 Butlletí +Kdades: Butlletí electrònic de tecnologia, auditoria i seguretat de la informació*, Nº. 24, 2013, pp. 7-8, acceso en http://dialnet.unirioja.es/servlet/extart?codigo=4329765.
82. MARTÍNEZ MARTÍNEZ, R. (2017) . Big data, investigación en salud y protección de datos personales ¿un falso debate?. *Revista Valenciana de Estudios Autonómicos*, nº 62. Recuperado de http://www.transparencia.gva.es/documents/19318353/165265446/RVEA+62+v2-1+Completo.pdf/791874c0-1290-4c34-9d27-51dbc520cb74
83. MARTÍNEZ MARTÍNEZ, R. (2017). Big data, investigación en salud y protección de datos personales ¿un falso debate?. *Revista Valenciana de Estudios Autonómicos*, nº 62, pp.239. En III Congreso Internacional sobre Protección de Datos de la Cátedra Google de Privacidad. Martínez, R. «Protección de datos y desarrollo tecnológico en un mundo global», en el BLOG LOPD y Seguridad. Recuperado de http://lopdyseguridad. es/proteccion-de-datos-y-desarrollo-tecnologico-en-un-mundo-global/
84. MARWALA, T., Xing, B. Blockchain and AI. University of Johannesburg. Recuperado de https://arxiv.org/ftp/arxiv/papers/1802/1802.04451.pdf
85. MAYER-SCHÖNBERGER et. Al. (mayo 2013). The Dictatorship of Data. *MIT Technology Review* . Recuperado de https://www.technologyreview.com/s/514591/the-dictatorship-of-

data/ acceso en español en https://www.technologyreview.es/s/3564/la-dictadura-de-los-datos (trad. Francisco Reyes).
86. MAYOR SERRANO, B. (2010). Alfabetización en salud.
87. MECHAS P, Lowe M, Gabriel S, Sikirica S, Sasane R, Arcona S (febrero de 2015). "Aumento de la participación del paciente en el desarrollo de fármacos". Biotecnología de la naturaleza . 33 (2): 134-5. doi : 10.1038 / nbt.3145 . PMID 25658275
88. MERTZ M., Jannes, M., Schlomann, A., Manderscheid, E., Rietz, C. y Woopen, C. 2016. *Digitale Selbstbestimmung* . Centro de Ética, Derechos, Economía y Social de Colonia Ciencias de la Salud. DOI 10.8716 / ceres / 00001
89. MUIR GRAY, J.A. (2011). *How to Get Better Value Healthcare*. Offox. Edic sec.
90. NICKOLSON PRICE, W. (2017) II . Regulating Black-Box Medicine" . *Michigan Law Review.* Recuperado de http://michiganlawreview.org/wp-content/uploads/2017/12/116MichLRev421_Price.pdf
91. NATHAN EAGLE, Alex (Sandy) Pentland (marzo de 2006). Realización de minería: detección de sistemas sociales complejos. Journal Personal and Ubiquitous Computing. Vol. 10, edic. 4, págs. 255-268. Shoshana Zuboff en *Big Other: vigilancia del capitalismo y las perspectivas de una civilización de la información*, Journal of Information Technology (2015) 30, pp. 75-89.
92. NIETO GALÁN, M.T. (2017). *Health: Registro médico electrónico en una red Blockhain.* (Trabajo fin de máster, Universidad Carlos III). Recuperado de https://e-archivo.uc3m.es/bitstream/handle/10016/26274/TFG_Maria-Teresa_Nieto_Galan.pdf?sequence=1&isAllowed=y.
93. NICOLÁS, P. *Congreso Big Data biosanitarios: Oportunidades e implicaciones jurídicas*. G.I. Cátedra de Derecho y Genoma Humano. Universidad del País Vasco UPV/EHU,8 y 9 de octubre de 2018.
94. NIETO GARRIDO, Eva, "Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad" Dtor. J.L. Piñar, 2016, en "Derecho a indemnización y responsabilidad". Página 555.
95. URIARTE LANDA, I. (2016).Ámbito de Aplicación material. En *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad.* Págs. 63-76. Dtor. Piñar Mañas. Madrid: Editorial Reus.
96. VALERO TORRIJOS, J. (2014) . Régimen Jurídico de la transparencia en el Sector Público: del Derecho de acceso a la reutilización de la información. En Cap. 19 *Acceso, reutilización y gestión avanzada de la información en el ámbito de la Administración sanitaria: implicaciones jurídicas desde la perspectiva y de la innovación tecnológica*. Editorial Aranzadi.
97. VAN ALSENOY (2012). Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC, *Computer Law & Security Review,* p. 40 en Converso, D.; "The accountability of data controllers in relation to Cloud providers". Tilburg University, Julio 2013. Recuperado de http://arno.uvt.nl/show.cgi?fid=131417
98. VÁSQUEZ ROCCA, A. Byung-Chul Han: La sociedad de la transparencia, autoexplotación neoliberal y psicopolítica. De lo viral-inmunológico a lo neuronal extresante. Nómadas. *Revista Crítica de Ciencias Sociales y Jurídicas*, N. 03. Universidad Complutense. Recuperado de hhttp://dx.doi.org/10.5209/NOMA.56074
99. VIDA-BOTA, J. Valores y principios de la dignidad humana y sus implicaciones éticas. Ver en *Asociación Catalana de Estudios Bioéticos.* Recuperado de

http://bioetica.cat/valores-y-principios-la-dignidad-humana-y-sus-implicaciones-eticas/?lang=es

100. VILLAREAL VALERA**, J**.A. (2015). Perspectiva sociológica de la salud como proceso socio cultural. *Revista Caribeña de Ciencias Sociales*. Recuperado de: http://www.eumed.net/rev/caribe/2015/12/salud.html
101. WANGM, Y. , KOSINSKI, M. (2018). Las redes neuronales profundas son más precisas que los humanos para detectar la orientación sexual a partir de imágenes faciales. *Journal of Personality and Social Psichology*. Recuperado de https://psyarxiv.com/hv28a/
102. WESTIN, A. F., (1967) Privacy and Freedom, New York, Atheneum, pág. 7. Vid. Saldaña, M. N., "La protección de la privacidad en la sociedad tecnológica..." op. cit. pág. 99.
103. WESTIN, A. F., 1967, Privacy and Freedom, New York, Atheneum, pág. 7. Vid. Saldaña, M. N., "La protección de la privacidad en la sociedad tecnológica..." op. cit. pág. 99
104. WARREN Samuel y BRANDEIS Louis, "The Right to Privacy", en The Harvard Law Review, No, 4, Boston, Harvard University, 1980. pp. 180 y ss., Edit. Civitas, edición a cargo de Benigno Pendás y Pilar Baselga, primera edición, Madrid, 1995, pp 22. Ver disponible en : http://www.law.louisville.edu/library/collections/brandeis/node/225
105. OHM, P. , (2010) . Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*. Vol. 57, p. 1701. Ver en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006
106. O'NEIL, C. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, New York: Crown.
107. PANG, Z., Tian, J., Chen, Q. (2014). Intelligent packaging and intelligent medicine box for medication management towards the Internet-of-Things. En *16th International Conference on Advanced Communication Technology*. Recuperado de http://ieeexplore.ieee.org/document/6779193/
108. PALM, E.. *Implicaciones e impacto de la poda de transacción de blockchain.* (Tesis de maestría, Luleå University of Technology 2017). Recuperado de http://www.diva-portal.org/smash/get/diva2:1130492/FULLTEXT01.pdfPEPPET, S.R. (2015) Regulation the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. *Texas Law Review*. Recuperado de http://www.texaslrev.com/wp-content/uploads/2015/08/Peppet-93-1.pdf
109. PÉREZ GÓMEZ, J.M. « La protección de los datos de salud », en A. RALLO LOMBARTE, R. GARCÍA MAHAMUT (coords.), *Hacia un nuevo derecho europeo de protección de datos*, Tirant lo Blanch, Valencia, 2015, pp. 629 y ss.
110. PEREZ, B., MUSOLEISi, M., STRINGHINI, G. *You are your Metadata: Identification and Obfuscation of Social Media Users using Metadata Information*. University College London. Recuperado de https://www.ucl.ac.uk/~ucfamus/papers/icwsm18.pdf
111. PEREZ LUÑO, A. E., Derechos Humanos, Estado de Derecho y Constitución, op. cit. pág. 330.
112. PIÑAR MAÑAS, J.L. (2016). Objeto del Reglamento. En *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad.* Págs. 51-62.Madrid: Editorial Reus
113. POLLITT, C. (2003). *The Essential Public Manager*. London: Open University Press/McGraw-Hill . En BOVENS, M. Analysing and Assessing Accountability: A conceptual Framework, 2006, p. 9 Recuperado de https://www.ihs.ac.at/publications/lib/ep7.pdf

114. PORTAL MANRUBIA, J.(2010) Publicación: *Revista Aranzadi Doctrinal* núm. 6/2010 parte Estudios. Editorial Aranzadi, S.A.U., Cizur Menor.
115. POLLEDO, J.J.F. (Septiembre 1997). El papel de las autoridades sanitarias ante los retos de la salud pública del S. XXI. Revista Española de Salud Pública. Vol. 71. No. 5. Madrid. Recuperado de http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1135-57271997000500001
116. PREUKSCHAT, A. (coord.); Kuchkovsky, C.; Gómez, G.; Diez, D.; Molero, Í.: (2017) *Blockchain: La revolución industrial de internet*. (pp.15). Barcelona: Edit Gestión2000.
117. PUYOL MONTERO, J.(2014).Una aproximación a Big Data. *Revista de Derecho UNED*, núm. 14, 2014, págs. 471-505.
118. PUYOL MONTERO, J. (20 de noviembre de 2016). ¿Qué es el "Data Governence o gobernanza de los datos"? *Confilegal*. Recuperado de https://confilegal.com/20161120-data-governance/
119. PUYOL MONTERO, Javier "Derecho a indemnización", Troncoso Reigada,Antonio (dir), "Comentarios a la LOPD, Civitas y Thomson-Reuters, Cizur Menor, pp. 1263 y ss.
120. KUAH Hon, W., Millard, C. Walden, I. (2012). Negotiating cloud contracts: Looking at clouds from both sides now. *Standford Technology Law Review.* Vol. 16. Number 1. Recuperado de http://stlr.stanford.edu/pdf/cloudcontracts.pdf
121. RABESS, Cecilia Esther (2014) Can big data be racist? *The Bold Italic*, http://www.theboldditalic.com/articles/4502-can-big-data-be-racistROUSE, M. (2015). IoMT or healthcare IoT. *IoT Agenda.* Recuperado de http://internetofthingsagenda.techtarget.com/definition/IoMT-Internet-of-Medical-Things
122. RALLO LOMBARTE, A., Estudios sobre la evolución del régimen sancionador en la legislación de protección de datos. *Revista de Estudios Políticos*, núm. 166, 2014, p. 116.
123. RIPOL CARULLA, S. (2016) Aplicación territorial del Reglamento. En *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad.* Págs. 77-95. Dtor. Piñar Mañas. Madrid: Editorial Reus.
124. REISMAN, D., Schultz, J., Crawford, K., Whittaker M. (abril 2018). Algorithmic Impact Assesments: A practica framework for public Agency Accountability. *AINow.* Recuperado de https://ainowinstitute.org/aiareport2018.pdf
125. ROMEO, C. M. (2009). La protección de datos de salud en la investigación biomédica. En C. Gómez-Piqueras, R. Martínez-Martínez, J. M. Pérez-Gómez, C. M., Romeo, J. Sánchez-Caro y N. Valcárcel, *Protección de datos e investigación biomédica*. Cizur Menor: Thomson Reuters Aranzadi.
126. RÖSSLER, B., 2005, The value of privacy, Cambridge: Cambridge Polity Press. Ver Thompson, J. B., "Los límites cambiantes de la vida pública y privada", op. cit. pág. 30.
127. RUBÍ, J. (2000). Los códigos tipo: la alternativa de la autorregulación. *Revista Actualidad Informática Aranzadi*, 35.
128. RUDNER, j, McDougall, C., Sailam, V. Smith, M., Sacchetii, A. (2016) Interrogation of patient smartphone activity tracker to assist arrhythmia management. *Annals of Emergency Medicine*. Recuperado de http://www.annemergmed.com/article/S0196-0644(16)00143-8/fulltext.
129. RULE, J. et al. (1983) . Documentary Identification and Mass Surveillance in the United States. *Social Problems* .Vol. 31. No. 2 pp. 222-234. Oxford Universtity Press. Recuperado de https://www.jstor.org/stable/800214?seq=1#page_scan_tab_contents
130. RUSSEL, Bertrand (2008). A Critical Exposition of the Philosophy of Leibniz . New York: Conimo Books, p. 192 en Steiner, C.. *Una breve historia de hombres y algoritmos*.

131. SANCHEZ LOSADA, J.A. (2011). *Aspectos éticos y médico-legales en la Telemedicina: la consulta médica telefónica.* (Tesis doctoral, Universidad Complutense). Pp. 18-9. Recuperado de http://eprints.ucm.es/13892/1/T33350.pdf
132. SCHUARTZ, Paul M. (2013) Information privacy in the cloud . *University of Pennsylvania Law Review*. Vol. 161. Págs. 1653-1661.
133. SETHL. et. Al. CRISPR–Cas encoding of a digital movie into the genomes of a population of living bacteriaRecuperado de https://www.nature.com/articles/nature23017.epdf?referrer_access_token=QTYFH4XLqouqTNuWD2ipqdRgN0jAjWel9jnR3ZoTv0MjdOpafyPGesq6gh7mzZ6ZdHcTUMneWjcfB2DFK1Zem8s314vA1wwtokTapzWH73tzibxm1DzcBduIq4HvsYvq6E25ebYf1JYZJ61ZxwofXsdZGwboJN-aOn4-FEG8WNKOjaloxKT4mPJGa
134. SIMACEK K, Raja P, Chiauzzi E, Eek D, Halling K (2017). "¿Qué esperan los pacientes de cáncer de ovario del tratamiento? Perspectivas de una comunidad de pacientes en línea". Enfermería Oncológica . 40 (5): E17 – E27. Doi : 10.1097 / NCC.0000000000000415 . PMID 27454765).
135. SINZIANA Mazilu et al., (2012) "Online Detection of Freezing of Gait with Smartphones and Machine Learning Techniques". Recuperado de: https://www.researchgate.net/publication/256503573_Online_Detection_of_Freezing_of_Gait_with_Smartphones_and_Machine_Learning_TechniquesSOLOVE, D. J., "A Taxonomy of Privacy", op. cit. pp. 523-548.
136. SOLOVE, D. J., 2008, Understanding Privacy, Cambridge, MA: Harvard University Press.
137. SOLOVE, D.J. (2013). Introduction: Privacy Self-Management and the Consent Dilemma. Recuperado de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018SPELBERG A., et al. (7 de febrero de 2017), Contribution of industry funded post-marketing studies to drug safety: survey of notifications submitted to regulatory agencies . *The bmj*. Recuperado en https://www.bmj.com/content/356/bmj.j337
138. SPINOZA, Baruch, *Ethics* , Libro III, página 2, nota; Libro II, página 48; Libro I, apéndice en Wikipedia.
139. STEINER (2012): Automate This: How Algorithms Came To Rule The World, *New York, Portfolio/ Penguin* en; Monasterio A. *Ética algorítmica: Implicaciones éticas de una sociedad cada vez más gobernada por algoritmos*, 2017.
140. STOWE S, HARDING S. (2010) Telecare, telehealth and telemedicine. *European Geriatric Medicine* ;1:193-7
141. STUART MILL, John, "*On Liberty. Prefaces to liberty*", Beacon Press, Boston, 1959SURDEN, H. (13 de marzo de 2017). Values Embedded in Legal Artificial Intelligence. *U of Colorado Law Legal Studies* Research Paper No. 17-17. Recuperado de https://ssrn.com/abstract=2932333 or http://dx.doi.org/10.2139/ssrn.2932333
142. SULLIVAN, C. , Burger, E. (2017) E-Residency and Blockchain. *Computer Law & Security Review* 460, 475. Recuperado de http://www.arifsari.net/isma500course/project/19.pdf
143. SWEENEY, L. (2013). Discrimination in online ad delivery. *Data Privacy Lab* http://dataprivacylab.org/projects/onlineads/1071-1.pdf
144. TAMÉS, A. (2018). Blockchain: La disrupción del rol del paciente en el ámbito de la salud. *Revista Sociedad Española de Informática de la Salud*. Pág. 8. Recuperado de https://seis.es/wp-content/uploads/2018/04/128.pdf
145. THOMPSON, J. B., "Los límites cambiantes de la vida pública y privada", op. cit. pág. 33.
146. TEIJEIRA, Mariano. Legal Compliance: Conceptualización en el marco de la regulación corporativa. En: Estudios sobre el futuro Código Mercantil: libro homenaje al profesor

Rafael Illescas Ortiz. Getafe : Universidad Carlos III de Madrid, 2015, pp. 935- 948. ISBN 978-84-89315-79-2. Recuperado de http://hdl.handle.net/10016/2102

147. TRANSBERG, P., HASSELBACH, G. (2018). DataEthics – Principles and Guidelines for Companies, Authorities & Organisation. Recuperado de https://dataethics.eu/wp-content/uploads/Dataethics-uk.pdf
148. TSAI, J. et. al. (2007). The Effect of Online Privacy Information on Purchasing Behaviour: An Experimental Study. Recuperado de https://www.econinfosec.org/archive/weis2007/papers/57.pdf
149. Valcárcel, N. (2009). Protección de datos de salud e investigación hospitalaria. En C. Gómez-Piqueras, R. Martínez-Martínez, J. M. Pérez-Gómez, C. M., Romeo, J. Sánchez-Caro y N. Valcárcel, *Protección de datos e investigación biomédica*. Cizur Menor: Thomson Reuters Aranzadi.
150. ZHENYU Chen et al., (2013) "Unobtrusive Sleep Monitoring Using Smartphones". Recuperado de https://ieeexplore.ieee.org/document/6563918.
151. ZETZSCHE DA Buckley RP, Arner DW (2017). The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain, *University of New South Wales Law Research Series*. Law Working Paper Series, Number 2017-007. Recuperado de http://dx.doi.org/10.2139/ssrn.3018214

INFORMES Y DOCUMENTACIÓN OFICIAL

152. GT29. Dictamen 4/2007 sobre el concepto de dato personal. Recuperado de https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf
153. GT29. Directrices sobre el consentimiento bajo la Regulación 2016/679 (WP259). Recuperado de https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051
154. GT29. Dictamen 03/2013 sobre la limitación de la finalidad. (WP 203). Recuperado de https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp203_en.pdf.
155. GT29. Dictamen 1/2010 de los conceptos responsible y encargado. (WP 169). Recuperado de https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf#page=26&zoom=100,0,694
156. GT29. Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE (WP 217)
157. GT29. Directrices sobre decisiones individuales automatizadas y perfilado (WP 251)
158. GT29. Dictamen 8/2014 sobre Desarrollos Recientes en Internet de las Cosas (WP 223). Recuperado de https://www.dataprotection.ro/servlet/ViewDocument?id=1088
159. GT29. Dictamen 5/2009 sobre redes sociales online (WP 163). Recuperado de http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf-
160. GT29. Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679. (WP 248). Recuperado de https://www.aepd.es/media/criterios/wp248rev01-es.pdf
161. COMISIÓN EUROPEA, The Future of Cloud Computing. Opportunities for European cloud computing beyond. Recuperado de http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf

162. COMISIÓN EUROPEA (6 de junio de 2017). European Data Market SMART 2013/0063 Final Report. Recuperado en https://ec.europa.eu/digital-single-market/en/news/european-data-market-study-data-related-health-tech-growing-fast
163. COMISIÓN EUROPEA (octubre 2018). Market study on telemedicine. Final Report. Recuperado en https://ec.europa.eu/health/sites/health/files/ehealth/docs/2018_provision_marketstudy_telemedicine_en.pdf
164. Comisión de las Comunidades Europeas (30 abril de 2004). La salud electrónica – hacia una mejor asistencia sanitaria para los ciudadanos europeos: Plan de acción a favor de un Espacio Europeo de la Salud Electrónica. (SEC(2004)539). Recuperado en http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52004DC0356&from=EN
165. COMISIÓN EUROPEA (6 de diciembre de 2012). Plan de acción sobre la salud electrónica 2012-2020: arLa salud electrónica – hacia una mejor asistencia sanitaria para los ciudadanos europeos: Plan de acción a favor de un Espacio Europeo de la Salud Electrónica. Ver en http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52012DC0736&from=EN
166. COMISIÓN EUROPEA (2018) . Consultation: Transformation Health and Care in the Digital Single Market. Recuperado en: https://ec.europa.eu/health/sites/health/files/ehealth/docs/2018_consultation_dsm_en.pdf.
167. COMISIÓN EUROPEA (25 de abril de 2018) Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society. Recuperado en https://ec.europa.eu/digital-single-market/en/news/communication-enabling-digital-transformation-health-and-care-digital-single-market-empowering.
168. COMISIÓN EUROPEA, Decisión de Ejecución (UE) 2016/2297 de 16 de diciembre de 2016 por la que se modifican las Decisiones 2001/497/CE y 2010/87/UE, relativas a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016D2297&from=ES
169. COMISIÓN EUROPEA (2014). Cloud Service Level Agreeement Standardisation Guidelines. Recuperado de https://ec.europa.eu/digital-single-market/en/news/cloud-service-level-agreement-standardisation-guidelines
170. Comunicación de la Comisión al Parlamento Europeo, al Consejo, Al Comité Económico y Social Europeo y al Comité de las Regiones. COM (2012) 529 final. "Términos y condiciones de contratación seguras y justas de la Estrategia Europea de Cloud Computing".
171. COMISIÓN EUROPEA (7 de junio de 2016). Digital Single Market. *Code of Conduct on privacy for mHealth apps has been finalised.* Recuperado de https://ec.europa.eu/digital-single-market/en/news/code-conduct-privacy-mhealth-apps-has-been-finalised
172. COMISIÓN EUROPEA (13 de septiembre 2017). Com (2017) 495 Final. Proposal for a Regulation of the European Parliament and of the council on a framework for the free flow of non-personal data in the European Union http://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-495-F1-EN-MAIN-PART-1.PDF
173. COMISIÓN EUROPEA (25 de abril 2018). Comunicación sobre la habilitación de la transformación digital de la salud y la atención en el mercado único digital. Empoderar a los ciudadanos y construir una sociedad más sana. Recuperado de https://ec.europa.eu/digital-

single-market/en/news/communication-enabling-digital-transformation-health-and-care-digital-single-market-empowering
174. COMISIÓN EUROPEA (Agosto 2013) Evaluation of the use and impact of the European Community Health Indicators ECHI by Member States. Final Report. Recuperado de https://ec.europa.eu/health/sites/health/files/indicators/docs/echi_report_v20131031.pdf
175. COMISIÓN EUROPEA (19 de diciembre de 2018). Draft Ethics Guidelines for Trustworthy AI. Recuperado de https://ec.europa.eu/knowledge4policy/publication/draft-ethics-guidelines-trustworthy-ai_en
176. COMISIÓN EUROPEA . Ethics Guidelines for Trustworthy AI. Recuperado de https://us18.campaign-archive.com/?u=a23897532dbb6100934258190&id=803e0320a1
177. COMISIÓN EUROPEA. (2018). Consultation: Transformation Health and Care in the Digital Single Market. Recuperado de https://ec.europa.eu/health/sites/health/files/ehealth/docs/2018_consultation_dsm_en.pdf
178. CONSEJO DE LA UE. Información procedente de las Instituciones, Órganos y Organismos de la UE. Conclusiones del Consejo sobre la salud en la sociedad digital: avanzar en la innovación basada en los datos en el ámbito de la salud (2017, C-440/05) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017XG1221(01)&from=ES
179. CONSEJO DE EUROPA. Comité de Ministros (27 de marzo de 2019). Recomendación CM/ Rec (2019) 2 del Comité de Ministros de los Estados Miembros sobre la protección de datos relacionados con la salud. Recueprado de https://search.coe.int/cm/pages/result_details.aspx?objectid=090000168093b26e
180. PARLAMENTO EUROPEO (20 de febrero de 2017). Propuesta de Resolución sobre las implicaciones de los macrodatos en los derechos fundamentales; privacidad, protección de de datos, discriminación, seguridad y aplicación de la ley. Recuperado de http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0044+0+DOC+XML+V0//ES
181. PARLAMENTO EUROPEO (21 de noviembre de 2013). Informe sobre sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)). Recuperado de http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//ES
182. PARLAMENTO EUROPEO (14 de marzo de 2017). Resolución sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI)) Recuperado de http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0076+0+DOC+PDF+V0//ES
183. SEPD (21 de mayo de 2015). Opinion 1/2015. Mobile Health. Reconciling technological innovation with data protection. Recuperado de https://edps.europa.eu/sites/edp/files/publication/15-05-21_mhealth_en_0.pdf
184. SEPD. Opinion 7/2015 Meeting the challenges of big data https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf
185. SEPD (2019). Opinion 3/2019 sobre las preguntas y respuestas sobre la interacción en el Reglamento de ensayos clínicos (CTR) y el RGPD. Recuperado de https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-32019-concerning-questions-and-answers-interplay_en

186. SEPD. Dictamen del 3/2017 sobre la Propuesta relativa a un Sistema Europeo de Información y Autorización de Viajes (ETIAS)
187. SEPD (2012) Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe". Recuperado de https://edps.europa.eu/sites/edp/files/publication/12-11-16_cloud_computing_en.pdf
188. SEPD (11 de septiembre de 2015) . Opinion 4/2015. Towards a new digital ethics. Data, dignity and technology. Recuperado de https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf
189. SEPD (25 de febrero de 2019). Directrices del SEPD para evaluar la proporcionalidad de las medidas que limitan los derechos fundamentales a la privacidad y la protección de datos personales. Recuperado de https://edps.europa.eu/data-protection/our-work/publications/guidelines/edps-guidelines-assessing-proportionality-measures_en
190. SEPD. Opinion 7/2015. Meeting the challenges of big data. A call for transparency, user control, data, protection by design and accountability. Recuperado de https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf
191. SEPD. (2015) Special Eurobarometer 431. Recuperado de http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_sum_en.pdfSEPD (23 de enero de 2019) . Dictamen 3/2019 relativo a las preguntas y respuestas sobre
192. la interacción entre el Reglamento sobre ensayos clínicos (CTR) y el Reglamento General de Protección de Datos (GDPR) (Art. 70.1.b)).Recuperado de https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf
193. OCDE (2017) Recomendación sobre Gobernabilidad de Datos de Salud.
194. COMITÉ INTERNACIONAL DE BIOÉTICA (15 de septiembre de 2017). *Informe del IBC sobre big data y salud.* Recuperado de http://unesdoc.unesco.org/images/0024/002487/248724e.pdf
195. UNIÓN EUROPEA (2012). eHealth Task Force Report. Redesigning health in Europe for 2020. https://datos.gob.es/es/documentacion/orientaciones-sobre-la-proteccion-de-datos-en-la-reutilizacion-de-la-informacion-del
196. WORLD HEALTH ORGANIZATION (2018). *Towards the Development of an mHealth Strategy: A Literature Review* pp 14. Recuperado en http://www.who.int/goe/mobile_health/mHealthReview_Aug09.pdf
197. ONU (2015). Informe del relator especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión. Recuperado de https://s3.amazonaws.com/s3.documentcloud.org/documents/2089684/un-encryption-report-special-rapporteur-on.pdf .
198. BOE, núm. 274, de 15 de noviembre de 1985. Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981.Recuperado de https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447.
199. AEPD. Directrices para la elaboración de contratos entre responsables y encargados del tratamiento. Recomendado de https://www.aepd.es/media/guias/guia-directrices-contratos.pdf.
200. AEPD. Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD. Recuperado de https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf
201. AEPD. Guía para el cumplimiento del deber de informar. Recuperado de https://www.aepd.es/media/guias/guia-modelo-clausula-informativa.pdf
202. AEPD. Resolución PS/00368/2015 R/02202/2015

203. AEPD. Protección de datos. Guía para el ciudadano. Recuperado de https://www.aepd.es/media/guias/guia-ciudadano.pdf
204. AEPD. Informe 073667/2018 del Gabinete Jurídico. Recuperado de https://www.aepd.es/media/informes/2018-0046-investigacion-biomedica.pdf
205. AEPD- UPM (2019) *Análisis de flujos de información en Android. Herramientas para el cumplimiento de responsabilidad proactiva*. Recuperado de https://www.aepd.es/media/estudios/estudio-flujos-informacion-android.pdf
206. AEPD. Novedades para el Sector Privado. Recuperado de https://www.aepd.es/media/docs/novedades-lopd-sector-privado.pdf
207. AEPD-ISMS Forum. Código de buenas prácticas em Protección de Datos para proyectos Big Data. Recuperado de https://www.aepd.es/media/guias/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf
208. AEPD. Guía evaluaciones de impacto. Recuperado de https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf
209. AEPD. Orientaciones y garantías en los procedimientos de Anonimización de datos personales. Recuperado de https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf
210. AEPD. Procedimiento Sancionador. R/02202/2015, PS/00368/2015.
211. AEPD. Procedimiento Sancionador PS/00368/2015 R/02202/2015
212. ACPD. Autoritad Catalana de Protección de Datos. (11 de enero de 2019). Resolución CNS 59/2018. Recuperado de http://apdcat.gencat.cat/web/.content/Resolucio/Resolucions_Cercador/Dictamens/Documents/ca_cns_2018_059.pdf
213. CIS. Barómetro de mayo 2018. Estudio n. 3213. Recuperado de http://datos.cis.es/pdf/Es3213mar_A.pdf
214. Decreto de Apertura (27 de marzo 2017) de Fiscalía Superior de la Comunidad Autónoma de Andalucía . Diligencias de Investigación Penal n.8/2017 (NGF 217/17). Recuperado de https://www.elconfidencialdigital.com/media/elconfidencialdigital/files/2017/04/08/ECDFIL20170408_0001.pdf

NORMATIVA

Normativa nacional

215. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Recuperado de https://boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf
216. Ley Orgánica 15/1999, de 13 de diciembre , de protección de datos de carácter personal. (derogada) Recuperado de http://noticias.juridicas.com/base_datos/Admin/lo15-1999.html
217. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. (Derogado) Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-2008-979

218. Ley 39/2015 de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565
219. LO 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Recuperado de http://noticias.juridicas.com/base_datos/Admin/lo1-1982.html
220. Ley 18/2015, de 9 de julio , por la que se modifica la reutilización de la información del sector público. Recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-7731
221. Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887
222. Decreto de 11 de noviembre de 1943 por el que se aprueba el Reglamento para la aplicación de la Ley del Seguro de enfermedad. Reglamento del Seguro de Enfermedad. Recuperado de https://www.boe.es/datos/pdfs/BOE//1943/332/A11427-11436.pdf
223. La Ley 14/1986, de 25 de abril, General de Sanidad. Recuperado de https://www.boe.es/buscar/doc.php?id=BOE-A-1986-10499
224. La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-2002-22188
225. La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud. Recuperado de . http://noticias.juridicas.com/base_datos/Admin/l16-2003.html#a1
226. La Ley 14/2007, de 3 de julio, de Investigación biomédica. Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-2007-12945
227. La Ley 33/2011, de 4 de octubre, General de Salud Pública. Recuperado de http://noticias.juridicas.com/base_datos/Admin/l33-2011.html
228. La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras. Recuperado de http://noticias.juridicas.com/base_datos/Fiscal/556605-l-20-2015-de-14-de-julio-de-ordenacion-supervision-y-solvencia-de-las-entidades.html
229. Real Decreto-ley de 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-2015-7897

Normativa comunitaria

230. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679
231. DOUE, 23 de mayo 2018. Corrección de errores del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD Recuperado de https://www.boe.es/doue/2018/127/L00003-00007.pdfhttps://www.boe.es/doue/2018/127/L00003-00007.pdf.
232. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos

personales y a la libre circulación de estos datos. Recuperado de https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML

233. Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DO L 194 de 19.7.2016, p. 1) (Directiva SRI).
234. Reglamento (UE) n.o 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (DO L 257 de 28.8.2014, p. 73) (Reglamento eIDAS). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32014R0910
235. Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas) (2018). Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017PC0010&from=LV
236. Directiva 2011/24 / UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, sobre la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza. Recuperado de https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32011L0024
237. Recomendación (UE) 2019/243 de la Comisión, de 6 de febrero de 2019, sobre un formato de intercambio de historiales médicos electrónicos de ámbito europeo.Recuperado de https://www.boe.es/buscar/doc.php?id=DOUE-L-2019-80241
238. Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la proteccion de las personas que informen sobre infracciones del Derecho de la Unión. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018PC0218&from=ES
239. Tratado de Lisboa por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea, Diario Oficial de la Unión Europea, C 306/1 DE 17 DE DICIEMBRE DE 2007. Accesible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A12007L%2FTXT
240. Comisión Europea (25 de enero de 2012). Comission Stadd Working Paper. Impact Assesment. Regulation of the European Paliament and of the Council on the protection of individuals with regard to the processing of personal data on the free movement of such data (RGPD) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data . Recuperado de https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0072&from=EN
241. Comunicación de la Comisión al Parlamento Europeo y al Consejo. Mayor protección, nuevas oportunidades: Orientaciones de la Comisión sobre la aplicación directa del Reglamento general de protección de datos a partir del 25 de mayo de 2018. Recuperado de https://ec.europa.eu/transparency/regdoc/rep/1/2018/ES/COM-2018-43-F1-ES-MAIN-PART-1.PDF
242. Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016L1148

243. Minister of Justice Canadá (2000). Personal Information Protection and Electronic Documents Act. Recuperado de http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf
244. Directiva 2001/20/CE del Parlamento Europeo y del Consejo, de 4 de abril de 2001, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros sobre la aplicación de buenas prácticas clínicas en la realización de ensayos clínicos de medicamentos de uso humano.
245. Reglamento (UE) nº 536/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, relativo a los ensayos clínicos de los medicamentos de uso humano y por la que se deroga la Directiva 2001/20/CE.
246. LOI n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé. Ley francesa de Modernización del Sistema de Sanidad. Recuperado de https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000031912641&categorieLien=id
247. Carta de los Derechos FundamentalesDeclaración Internacional de Ética y Protección de datos en IA .Recuperado de https://www.privacyconference2018.org/system/files/2018-10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf

JURISPRUDENCIA

Jurisprudencia nacional

248. Sentencia del Tribunal Constitucional 254/1993, de 20 de julio de 1993. Recuperado de http://hj.tribunalconstitucional.es/it/Resolucion/Show/2383
249. Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre de 2000. Recuperado de http://hj.tribunalconstitucional.es/es/Resolucion/Show/4276
250. Sentencia del Tribunal Constitucional 202/1999, de 8 de noviembre.
251. Sentencia del Tribunal Constitucional 94/1998, de 4 de mayo.
252. Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre.
253. Sentencia del Tribunal Constitucional 11/1998, FJ 5, 94/1998, FJ 4.
254. Sentencia del Tribunal Constitucional 65/196, de 22 de Mayo.
255. Sentencia del Tribunal Constitucional 160/1987, de 27 de octubre.
256. Sentencia del Tribunal Supremo, Sala de lo C.A. 3896/2014, de 3 de Octubre de 2014, Rec 6153/2011. Recuperado de http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=7195354&links=&optimize=20141023&publicinterface=true
257. Sentencia del Tribunal Supremo 469/1997, de 31 de mayo, o 498/1993, de 18 de mayo, SSTS 799/2002, de 26 de julio
258. Sentencia del Tribunal Supremo 532/2015, de 23 de septiembre
259. Sentencia del Tribunal Supremo de 16 de marzo de 2016, Sala Primera, ponente Magistrado Rafael Saraza Jimena, recurso de casación núm. 3269/2014
260. Sentencia del Tribunal Supremo de 5 de junio de 1998
261. Sentencia de la Audiencia Nacional, Sala de lo Contencioso-administrativo, Sección 1ª, 20 sep. 2002 (Rec. 150/2000).
262. Sentencia de la Audiencia Nacional, Sala de lo Contencioso-administrativo, Sección 1ª, 16 mar. 2006 (Rec. 427/2004).

263. Sentencia de Audiencia Nacional (Sala de lo Contencioso-Administrativo, Sección 1ª, de 26 de abril de 2012. Recuperado de http://cooperacionconcellos.deputacionlugo.org/portal_localweb/RecursosWeb/DOCUMENTOS/1/0_2578_1.pdf
264. Sentencia Tribunal Superior de Justicia de Navarra 2/2012, de 8 de febrero de 2012. Recuperado en http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=6283325&links=servicio%20navarro%20de%20salud&optimize=20120225&publicinterface=true
265. Sentencia Penal Nº 892/2015, Audiencia Provincial de Barcelona, Sección 7, Rec 23/2015 de 26 de Noviembre de 2015
266. Sentencia Penal Nº 144/2018, Audiencia Provincial de Lleida, Sección 1, Rec 233/2017 de 03 de Abril de 2018
267. Sentencia Penal Nº 892/2015, Audiencia Provincial de Barcelona, Sección 7, Rec 23/2015 de 26 de Noviembre de 2015
268. Sentencia de la Audiencia Nacional 437/2008, de 27 de febrero de 2008. Recuperado en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=181372&statsQueryId=104385084&calledfrom=searchresults&links=&optimize=20080403&publicinterface=true
269. Sentencia Audiencia Provincial de Murcia 106/2008, de 13 marzo. (Sección 1ª). AC 2008\978. Jurisdicción: Civil. Recurso de Apelación núm. 296/2007.
270. Sentencia de la Audiencia Provincial de Alicante, sec. 8ª, S 13-11-2007, nº 423/2007, rec. 342/2007.

Jurisprudencia comunitaria

271. Sentenia del Tribunal de Justicia de la Unión Europea, caso *Bodil Lindqvist,* demanda núm. C-101/01, Sentencia de 6 de noviembre de 2003, p.29. Accesible en : https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62001CJ0101&from=EN
272. Sentenia del Tribunal de Justicia de la Unión Europea, caso *Eugen Schmidberger, Internationale Transporte und Planzüge contra Republic Österreichm ¡,* demanda núm. C-112/00, Sentencia de 6 de noviembre de 2003, p. 80. Accesible en : http://curia.europa.eu/juris/liste.jsf?language=en&num=C-112/00
273. Sentencia del Tribunal de Justicia de la Unión Europea, Sala 2ª. Asunto C-582/14, de 19 de octubre de 2016. Recuperado de http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=1314731
274. Sentencia del TEDH. Sentencia 28341/95, DE 4 DE MAYO DE 2000. Caso Rotaru contra Alemania. Derecho al respeto de la vida privada. Recuperado de http://hudoc.echr.coe.int/eng?i=001-162581
275. Sentencia del Tribunal de Justicia de la Unión Europea Breyer v. Alemania, C-582/14, § 31, 39 (ECJ 2016)- Recuperado de http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN
276. Sentencia asunto C-255/14
277. Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, *Google Spain* y Agencia Española de Protección de Datos, asunto C13/12

278. Sentencia del TJUE de 13 de mayo de 2014. Recuperado de http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES
279. Asuntos acumulados C-293/12 y C-594/12, ECLI:EU:C:2014:238.
280. Asuntos acumulados C-465/00, C-138/01y C-139/01, Rechnungshof, ECLI:EU:C:2003:294,
281. Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de noviembre de 2003. Asunto C-101/01. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62001CJ0101&from=EN

Jurisprudencia extranjera

282. Sentencia del Tribunal de Milán de 13 de febrero de 2008 (sección VIII de lo Civil. Stc N. 1774
283. Sentencia del Tribunal Supremo de los EEUU Whalen v. Roe (1977) 429. U.S. 589, sobre protección de datos persobales. Traducido por E. Guillén López. Recuperado de: http://www.ugr.es/~redce/REDCE7/articulos/16sentenciasupremoamericano.htm

TABLAS E IMÁGENES

Tablas

Imágenes

RECURSOS ELECTRÓNICOS

430. La ética del Diseño: Hacia un sistema más sustentable y responsable. *Conference: 3er. Congreso Internacional de Bioética*, At Toluca, Estado de México. Recuperado de https://www.researchgate.net/publication/274638707_La_etica_del_Diseno_Hacia_un_sistema_mas_sustentable_y_responsable?enrichId=rgreq-c4338b7ff3468407ed016a5be2e5facd-XXX&enrichSource=Y292ZXJQYWdlOzI3NDYzODcwNztBUzoyMTU3Mzg2MDc1MDk1MDRAMTQyODQ0NzUwMDkyOQ%3D%3D&el=1_x_3&_esc=publicationCoverPdf
431. *Revista de la Sociedad Española de Informática y Salud*. Número 128. Abril 2018. Blockchain en Salud. ¿Quimera o realidad?. Recuperado de https://seis.es/wp-content/uploads/2018/04/128.pdf
432. Grupo de trabajo sobre big data, de la Comisión de investigación de nuevas tecnologías del Centro Superior de Estudios de la Defensa Nacional (Ceseden) (2013) . Big Data en los entornos de defensa y seguridad. Documento de investigación 3/2013. Pág. 9.
433. Garcia, L. (20 enero 2018). ¿Cómo diagnosticar enfermedades a través de la forma del rostro? *SaludDigital*. Recuperado de https://www.consalud.es/saludigital/94/como-diagnosticar-enfermedades-a-traves-de-la-forma-del-rostro_45763_102.html
434. Quijije, J. (17 julio 2017). Crean el primer dispositivo médico en el mundo basado en tecnología Blockchain. *Coincrispy*. Recuperado de https://www.coincrispy.com/2017/07/17/bowhead-dispositivo-blockchain/
435. http://www.fundacioneconomiaysalud.org/wp-content/uploads/2015/07/100-PERSPECTIVAS-PARA-MEJORAR-EL-FUTURO-DEL-SECTOR-SALUD-Fundacion-Economia-y-Salud.pdf
436. Ash, S. (25 de mayo de 2016). The value of patient data. *Pwc Uk Blogs*. Recuperado en https://pwc.blogs.com/health_matters/2016/05/the-value-of-patient-data.html
437. Transparency Market Research (2018). Global Digital Health Market. Recuperado en https://www.transparencymarketresearch.com/digital-health-market.html
438. Federación de Asociaciones para la Defensa de la Sanidad Pública (19 agosto 2017). La enfermedad, un negocio para la industria farmacéutica. *Nueva Tribuna.es*. Recuperado en https://www.nuevatribuna.es/articulo/sanidad/enfermedad-negocio-industria-farmaceutica/20150302105350113131.html
439. IM Farmacias (24 de mayo de 2018. El mercado farmaceutico crece un 1,3% de facturación. Recuperado en https://www.imfarmacias.es/noticia/15355/el-mercado-farmaceutico-crece-un-13-en-facturacion
440. Simón Ruiz, A. (28 de junio de 2018). Los pagos de las farmacéuticas a los médicos se disparan un 12% hasta 564 millones. *CincoDías*. Recuperado en https://cincodias.elpais.com/cincodias/2018/06/28/companias/1530186688_725021.html
441. EFE Nueva York (18 de febrero de 2016). Ibm desembolsará 2.300 millones por la empresa de datos Truven Health Analytics. *Expansión.* (Recuperado en http://www.expansion.com/empresas/tecnologia/2016/02/18/56c5eae5268e3ed4668b46b1.html

Web de Singularity University; https://su.org/

443. Web The Medical Futuristic Institute (Dr. Meskò Bartalan). Recuperado en http://tmfinstitute.org/
444. Redacción Consalud (15 de mayo de 2018). Un nuevo estetoscopio revoluciona el uso de los teléfonos inteligentes.*Consalud.es*.Recuperado en https://www.consalud.es/tecnologia/nuevo-estetoscopio-revoluciona-el-uso-de-los-telefonos-inteligentes_50170_102_amp.html
445. Siwicki, B. (2 de octubre de 2017). "Traiga sus propios datos" en la próxima tendencia en salud. *Healthcare IT News.* Recuperado en http://www.healthcareitnews.com/news/bring-your-own-data-next-trend-healthcare
446. Organización Mundial de la Salud (OMS) . *Preventing chronic diseases: a vital investment*. Recuperado en http://apps.who.int/iris/bitstream/10665/43314/1/9241563001_eng.pdf
447. https://www.fundacionbankinter.org/documents/20183/97216/Salud++Digital+ES/5f5bd348-ca10-49de-8bfe-2ba368a2e269 . Pág. 40, 50.
448. Andrus Ansip; Comisión Europea (20 de abril de 2018). Making digital technology work for healthy livind. *Blog Post European Commission*. Recuperado en https://ec.europa.eu/commission/commissioners/2014-2019/ansip/blog/making-digital-technology-work-healthy-living_en
449. http://www.pardell.es/el-estandar-hl7.html
450. AEPD (octubre de 2010). *Informe de cumplimiento de la LOPD en Hospitales*. Recuperado en http://www.herbogeminis.com/IMG/pdf/aepd2.pdf.
451. http://www.dailymail.co.uk/news/article-1211037/Internet-doctor-prescribed-drugs-suspended-struck-off.html
452. SaludDigital (5 de mayo de 2018). Telepediatría en las escuelas para ahorrar visitas al médico. *SaludDigital Atención Sanitaria*. Recuperado de https://www.consalud.es/saludigital/109/telepediatria-en-las-escuelas-para-ahorrar-visitas-al-medico_49993_102.html
453. SaludDigital. Ejemplos para entender la Salud Digital (III): Organizaciones sanitarias. 3. Innovación en Organizaciones sanitarias. Recuperado en https://saludconectada.com/salud-digital-innovacion-organizaciones/.
454. https://www.consalud.es/saludigital/116/un-sistema-monitoriza-la-salud-de-los-ancianos-en-sus-domicilios_51954_102.html
455. Jiménez, I (28 de abril de 2018). Cumpliendo con la GDPR. *Abogacía Española Consejo General. Blogs*. Recuperado en https://www.abogacia.es/2018/04/26/cumpliendo-con-la-gdpr/
456. Patient View (2012). *European Directory of Health Apps 2012-2013. A review by patient groups and empowered consumers.* Recuperado en http://www.patient-view.com/uploads/6/5/7/9/6579846/pv_appdirectory_final_web_300812.pdf
457. http://www.azumio.com/apps/heart-rate/
458. Leon, N & Schneider H. (2012) *MHealth4CBS in South Africa: a review of the role of mobile phone technology for monitoring and evaluation of community based health services, South African Medical research services and the University of the Western Cape.* Recuperado de http://www.hst.org.za/publications/NonHST%20Publications/MHealth4CBS-A%20Review.pdf
459. http://computerhoy.com/noticias/hardware/hombre-implanta-chip-nfc-su-propia-mano-20035
460. https://www.clarin.com/sociedad/3000-suecos-implantaron-chip-electronico-datos-piel_0_rJkfU2rCf.htm
461. ONTSI (2015). Estudio sobre opiniones y expectativas de los ciudadanos sobre el uso y la aplicación de las TI en el ámbito sanitario. Recuperado de http://www.ontsi.red.es/ontsi/sites/ontsi/files/los_ciudadanos_ante_la_e-sanidad.pdf.
462. Horihuela, J. (23 de febrero 2018) Health care in 2030: AI And the Shifting Role Of Your Pharmacist. *Forbes.* Recuperado de https://www.forbes.com/sites/forbestechcouncil/2018/02/23/health-care-in-2030-ai-and-the-shifting-role-of-your-pharmacist/#104f13d032c5
463. https://es.wikipedia.org/wiki/Industria_farmac%C3%A9utica
464. Champagne, D., Hung, A., Leclerc, O. (dic. 2015). Cómo las farmacias pueden ganar en un mundo digital. *Blog McKinsey & Company Productos farmaceuticos y productos médicos.* Recuperado de

https://www.mckinsey.com/industries/pharmaceuticals-and-medical-products/our-insights/how-pharma-can-win-in-a-digital-world
465. https://www.mckinsey.com/industries/pharmaceuticals-and-medical-products/our-insights
466. http://www.proteus.com/discover/
467. Van Den Heuvel, R. (6 de febrero de 2017). Pharma outlook 2030: From evolution to revolution. *KMPG*. Recuperado de: https://home.kpmg.com/xx/en/home/insights/2017/02/pharma-outlook-2030-from-evolution-to-revolution.html?cid=linkd_soc_xx-acx_adv-pharma2030&utm_medium=soc&utm_source=linkd&utm_content=xx-acx&utm_campaign=adv-pharma2030&sf54814790=1
468. Cachafeiro Jardón, M.J. (2018). La FarmAPPedia. *Catálogo de APPs de uso y preescripción en la Farmacia*. Recuperado de https://www.dropbox.com/s/wzs44nnkh30gz4g/La%20FarmAPPedia.pdf?dl=0
469. RedacciónMédica (15 de noviembre de 2017). Nuevo código de la industria para proteger datos personales en "Big Data". *Redacción Médica.* Ver en: https://www.redaccionmedica.com/secciones/industria/nuevo-codigo-de-la-industria-para-proteger-datos-personales-en-big-data--8696
470. S.Nadal, MV (26 de diciembr de 2018). Algoritmos para acelerar la investigación de fármacos. Retina *El País Economía.* Recuperado de https://retina.elpais.com/retina/2018/12/21/innovacion/1545388739_968425.html?Id_externo_rsoc=TW_CM_RT_bc_phm
471. www.mendelian.co
472. Palomas D. (20 de abril de 2018). ¿Cuál es el coste de desarrollar nuevos medicamentos?. *Dciencia.* Recuperado de http://www.dciencia.es/cual-es-el-coste-de-desarrollar-nuevos-medicamentos/
473. https://medrec.media.mit.edu/
474. Oliva, F., Flores, M. La transformación de las compañías de seguros en la era digital. *Deloitte Análisis*. Recuperado de https://www2.deloitte.com/uy/es/pages/strategy-operations/articles/La-transformacion-de-las-companias-de-seguros-en-la-era-digital.html
475. https://nae.global/posicionamiento-digital-de-las-aseguradoras-generales-en-espana-i/
476. Reuters (20 de septiembre de 2018). Sin pulsera de actividad no hay seguro de vida, la nueva estrategia aseguradora en EEUU. *El Economista.* Recuperado de https://www.eleconomista.es/empresas-finanzas/noticias/9400218/09/18/Sin-pulsera-de-actividad-no-hay-seguro-de-vida-la-nueva-estrategia-aseguradora-en-EEUU.html
477. https://www.vivaz.com/politica-de-privacidad-ampliada.html
478. Del Valle, M, (2014) La computación en la nube en Europa y en España: una oportunidad de negocio. Folleto *DELL EMC*. Recuperado de https://www.dellemc.com/es-es/solutions/storage/ecs/cloud-services-simple-storage.htm
479. Hon, K. (16 de junio de 2015). Cloud Security under the Data Protection Directive and Draft General Data Protection Regulation. En *ENISA EU28 Cloud Security Conference*. Recuperado de https://www.enisa.europa.eu/events/enisa-events/cloud-security-conference-reaching-the-cloud-era-in-the-eu/speakers-images/HonENISACloudSecurityDataProtection-distribution.pdf
480. https://tecnologiaparatuempresa.ituser.es/cloud/2019/02/tendencias-que-influiran-en-el-mercado-saas-en-2019
481. http://www.computerworld.es/pubs/cw1336/files/35.html
482. https://www.revistacloudcomputing.com/2018/10/blockchain-al-servicio-de-un-nuevo-mercado-de-almacenamiento/
483. Trenholm, R. (30 de noviembre de 2016). Lucha contra el jet-lag: la píldora digital le dice a la tripulación de cabina lo que necesitas. *CNET*. Recuperado de https://www.cnet.com/news/fight-jet-lag-with-the-digital-pill-that-tells-cabin-crew-what-you-need/
484. Frost &Sullivan (27 de junio de 2017). *¿Es IoMT la solución mágica para remodelar la prestación de la atención coordinada y proactiva?* Recuperado de https://ww2.frost.com/news/press-releases/iomt-magic-bullet-reshape-coordinated-and-proactive-care-delivery/

485. Crawford, K. (nov 2014). When Fitbit Is the Expert Witness. *The Atlantic*. Technology. Recuperado de https://www.theatlantic.com/technology/archive/2014/11/when-fitbit-is-the-expert-witness/382936/
486. Villariño, A. (Andrés Vilariño). (29 de Marzo de 2019). Recuperado de https://twitter.com/andresvilarino/status/1111781345481629696.
487. Comstock, J. (16 de noviembre de 2012). FDA aprueba el termómetro corporal con capacidad para Iphone. *Mobihealthnew*s . Recuperado de http://mobihealthnews.com/19110/fda-clears-iphone-enabled-body-thermometer/
488. Nobbot (3 de enero de 2019). Investigadores de IBM sacan las uñas para luchar contra el Parkinson. *Editorial Nobbot.* Recuperado de https://www.nobbot.com/general/ibm-sensor-de-unas/
489. Cadie Thompson (2013). The Future of Medicine Means Part Human. Part Computer, *CNBC*. Recuperado en http://www.cnbc.com/id/101293979.
490. Vid. http://www.givenimaging.com/enus/Innovative-Solutions/Capsule-Endoscopy/Pages/default.aspx
491. Vid. http://givenimaging.com/en-us/InnovativeSolutions/Motility/SmartPill/Pages/default.aspx
492. Vid. http://www.proteus.com/ technology/digital-health-feedback-system/ç
493. Dans. E. (2017). Devorando sensores: el futuro de la medicina. Recuperado de https://www.enriquedans.com/2017/11/devorando-sensores-el-futuro-de-la-medicina.html
494. Ross Brooks (2013) Tooth-Embedded Sensor Relays Eating Habits to the Dentist, *PSFK* http://www.psfk.com/2013/07/tooth-sensor-track-eating-habits.html
495. Nobbot (3 de enero de 2019). Investigadores de IBM sacan las uñas para luchar contra el parkinson. *Editorial Nobbot*. https://www.nobbot.com/general/sensor-diente-rastrea-comida/
496. https://youtu.be/DTXqUrmr3FQ
497. Villariño, A. (29 de marzo de 2019) Recuperado de https://twitter.com/andresvilarino/status/1111694528438771712. "This Futuristic #ESkin Can Monitor Your #Health Remotely. via @DigitalMedDoc"
498. http://www.bioe.umd.edu/news/news_story.php?id=10234
499. http://www.bioe.umd.edu/sites/default/files/images/011717-figure.jpg
500. https://www.eleconomista.es/empresas-finanzas/noticias/8224842/03/17/Cuando-los-vibradores-te-espian-multa-de-4-millones-a-una-empresa-que-registraba-el-uso-de-sus-consoladores.html
501. http://www.heatherpatterson.org/
502. http://bit.ly/2dhGc89
503. https://globalchallenge.virginpulse.com
504. Kaivan Karimi (2013) "The role of sensor fusion and remote emotive computing (REC) in the IoT". Recuperado de https://cache.freescale.com/files/32bit/doc/white_paper/SENFEIOTLFWP.pdf.
505. Lecuit, J.A. (23 de abril de 2018) . Cifrado, IoT y RGPD: tres desafíos de ciberseguridad en 2018. Real *Instituto El Cano Royal Institute.* Recuperado de http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=%2Felcano%2Felcano_es%2Fzonas_es%2Fari56-2018-alonsolecuit-cifrado-iot-rgpd-tres-desafios-ciberseguridad-2018&
506. https://www.consalud.es/saludigital/113/nuevo-sistema-basado-en-analisis-de-datos-para-tratamientos-individualizados-contra-el-cancer_51118_102.html
507. https://www.consalud.es/saludigital/105/el-big-data-llega-a-la-induccion-al-parto_48900_102.html
508. ICO (4 de septiembre de 2017). Big data, artificial intelligence, machine learning and data protection. Recuperado de https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf
509. Soares, S. (3 de junio de 2012). Not your type? Big Data Matchmaker on five data types you need to explore today. *Dataversity*. Vid. http://www.dataversity.net/not-your-type-big-data-matchmaker-on-five-data-types-you-need-to-explore-today/
510. https://www.eureporter.co/health/2017/05/05/eapm-meps-urge-commission-to-ramp-up-big-data-initiatives-in-health-care/
511. http:// www.nasonline.org/programs/sackler-colloquia/ completed_colloquia/Big-data.html
512. https://wellcome.ac.uk/sites/default/files/wtp053205_0.pdf

513. Nuffield Council on Bioethics (2015). *La recopilación, vinculación y uso de datos en biomedicina investigación y cuidado de la salud: cuestiones éticas*. Recuperado de http://nuffieldbioethics.org/wp-content/uploads/Biological_and_health_data_web.pdf
514. https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment
515. https://www.youtube.com/watch?v=716SW-TS71w
516. https://www.marketingweek.com/2015/07/08/consumers-are-dirtying-databases-with-false-details/
517. Taneja, H. (8 de septiembre de 2016). The need for algorithmic accountability. *TechCrunch.* Recuperado de https://techcrunch.com/2016/09/08/the-need-for-algorithmic-accountability/
518. D'Acquisito, Giuseppe et al. (diciembre 2015) Privacy by design in big data. An overview of privacy
519. enhancing technologies in the era of big data analytics. *ENISA*. Recuperado de https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/big-dataprotection
520. http://ukanon.net/
521. https://adrn.ac.uk/protecting-privacy/
522. http://dynamicinsights.telefonica.com/488/smart-steps
523. Fundación Vodafone España y Red. Es. *Big data en salud digital.* Informe de resultados. Recuperado de http://www.fundacionvodafone.es/sites/default/files/informe_big_data_en_salud_digital.pdf pp.22
524. https://www.withings.com/us/en/blood-pressure-monitor
525. https://www.xataka.com/robotica-e-ia/pillo-es-robot-asistente-que-mira-por-tu-salud-reconoce-caras-y-dispensa-medicamentos
526. https://m.xataka.com/inteligencia-artificial/compania-china-proporciona-consultas-medicas-sustituyendo-personal-medico-asistentes-virtuales/amp.
527. https://www.linkedin.com/feed/update/urn:li:activity:6517335238446714880/
528. https://www.wired.com/insights/2014/12/wearing-your-intelligence/
529. https://www.merca2.es/la-inteligencia-artificial-cuidado-medico/
530. https://wwwhatsnew.com/2017/11/17/este-algoritmo-puede-detectar-neumonia-con-mas-precision-que-un-radiologo/?utm_source=dlvr.it&utm_medium=twitter
531. https://news.aamc.org/research/article/artificial-intelligence-transforms-future-medicine/
532. https://www.nature.com/articles/srep26094
533. https://www.consalud.es/saludigital/112/nuevo-algoritmo-de-ia-para-detectar-enfermedades-oculares_50701_102.html
534. https://www.consalud.es/saludigital/134/facebook-crea-una-base-de-datos-de-imagenes-de-resonancias-magneticas_57657_102.html
535. https://unclineberger.org/
536. https://www.nature.com/articles/s41746-019-0096-y
537. BBC (1 de noviembre de 2016). Los algoritmos ocultos que funcionan como "armas de destrucción matemática. *BBC news.* Recuperado de http://www.bbc.com/mundo/noticias-37837377.
538. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-be-subject-automated-individual-decision-making-including-profiling_es
539. Burlacu, A. (12 de agosto de 2018). Understanding a Black-Box. *Towards Data Science*. Recuperado de https://towardsdatascience.com/understanding-a-black-box-896df6b82c6e
540. https://www.regulations.gov/document?D=FDA-2019-N-1185-0001
541. https://www.statnews.com/2019/04/02/fda-new-rules-for-artificial-intelligence-in-medicine/
542. https://www.consalud.es/saludigital/109/blockchain-pieza-clave-para-nuestra-salud_49823_102.html
543. http://curaesalud.com/wp-content/uploads/2017/09/Guia-Blockchain-para-el-sector-de-la-salud-Curaesalud.pdf
544. PwC (2013). Kosten im Gesundheitswesen: Durch Digitalisierung über CHF 100 Mio. einsparen. Recuperado de https://www.swisscom.ch/de/about/medien/press-releases/2014/09/20140902-MM-KostenGesundheitswesen.html
545. Scheuer, E. (2018). Whitepaper HIT Foundation HIT Foundation Zug. Recuperado de https://hit.foundation/wp-content/uploads/whitepaper-hit-foundation-v2.pdf
546. Independent (2017). *NHS cyber attack: Large-scale hack plunges hospitals across England into chaos.* Recuperado de http://www.independent.co.uk/news/uk/home-news/nhs-cyber-attack-hospitals-hack-englandemergency-patients-divert-shut-down-a7732816.html

547. https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data
548. https://www.pointnurse.com/blog/do-you-have-a-healthcare-blockchain-strategy/
549. https://www.eleconomista.es/economia/noticias/8899454/01/18/Hyperledger-la-Blockchain-privada-que-todos-tenemos-que-conocer.html
550. https://medium.com/@_mtnieto/creando-una-red-privada-blockchain-con-hyperledger-fabric-2e1567167325
551. https://retina.elpais.com/retina/2018/12/21/innovacion/1545388739_968425.html?Id_externo_rsoc=TW_CM_RT_bc_phm
552. http://ehealthreporter.com/es/noticia/blockchain-una-tecnologia-que-revolucionara-la-salud/
553. https://www.beckershospitalreview.com/lists/25-blockchain-companies-in-healthcare-to-know-2017.html
554. https://zenome.io/
555. Jones, B. (13 de septiembre de 2017). 23 andMe is Raising 200 millones de dólares al hacer medicamentos desde tu ADN. *Futurism*. Recuperado de https://futurism.com/23andme-is-raising-200-million-to-make-drugs-from-your-dna/
556. https://communityofinsurance.es/blog/2018/02/25/blockchain-y-seguro/#1519579978160-bb60bc98-c05c
557. https://www.vivaz.com/app/actividad.html
558. https://www2.deloitte.com/uy/es/pages/strategy-operations/articles/La-transformacion-de-las-companias-de-seguros-en-la-era-digital.html
559. https://nem.io/technology/
560. https://hit.foundation/wp-content/uploads/Whitepaper-HIT-Foundation.pdf
561. http://www.expansion.com/empresas/banca/2018/04/10/5accd666ca4741fa528b4635.html
562. https://www.xataka.com/internet-of-things/iota-la-criptomoneda-sin-blockchain-que-ha-crecido-un-1000-en-un-mes
563. CNIL. Recommendations for companies planning to use Cloud computing services. Recuperado de https://www.cnil.fr/sites/default/files/typo/document/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf
564. https://cloudsecurityalliance.org/
565. https://www.caprivacy.org/
566. https://ec.europa.eu/digital-single-market/
567. Cloud Industry Forum, Cloud UK. (2011) Paper Three – *Contracting Cloud Services: A Guide to Best Practices.* Recuperado de http://www.cloudindustry forum.org/downloads/whitepapers/cif-white-paper-1-2011-cloud-uk-adoption-andtrends.pdf
568. Hall, K. (19 de septiembre de 2011). Warwickshire County Council Signs Google to Pilot G-Cloud Email Service. *Computerweekly*. Recuperado de http://www. computerweekly.com/news/2240105636/Warwickshire-County-Council-signs-Google-topilot-G-Cloud-e-mail-service
569. http://www.ciospain.es/seguridad/nueva-ley-de-proteccion-de-datos-de-la-ue-donde-estan-las-dificultades-para-cumplirla
570. https://anf.es/pdf/MODELO-DEFINITIVO-AEPD_Contrato-encargado-subencargado-21-03-2012.pdf
571. Pérez Campillo, L. (12 de diciembre de 2016). Cloud Computing: Gestión de riesgos y data protection; ¿cómo evitar pagar los platos rotos? *ItUser*. Recuperado de https://www.ituser.es/opinion/2016/12/cloud-computing-gestion-de-riesgos-y-data-proteccion-como-evitar-pagar-los-platos-rotos
572. https://www.ismsforum.es/ficheros/descargas/acuerdo-de-nivel-de-privacidad1374159133.pdf
573. http://www.cloudcarib.com/
574. González, P.A. (2015). Privacidad en la Internet de las Cosas. Recuperado de https://www.slideshare.net/pagonzalez/privacidad-en-la-internet-de-las-cosas-presentacin
575. https://www.clarin.com/sociedad/lentes-inteligentes-ciegos-realidad-venden-varios-paises_0_HyxEvbOHb.html

576. https://os.kaspersky.com/wp-content/uploads/sites/11/2018/04/Kaspersky-IoT-security-whitepaper_print.pdf
577. https://www.xataka.com/wearables/estas-gafas-inteligentes-toshiba-dynaedge-dispositivo-reconocimiento-facial-basado-windows
578. https://communityofinsurance.es/blog/2017/11/19/asi-impacta-el-internet-de-las-cosas-en-el-sector-asegurado/
579. https://newsroom.uhc.com/
580. https://www.inithealth.com/en/
581. https://www.ca.com/en/blog-highlight/apis-for-your-ehr.html
582. https://bluebutton.cms.gov/
583. https://www.transparencymarketresearch.com/healthcare-api-market.html
584. https://clipset.20minutos.es/una-aseguradora-quiere-implantar-el-apple-watch-como-regalo-para-sus-clientes/
585. https://blog.puntoseguro.com/reto-puntoseguro-seguros-que-te-recompensan-por-estar-sano/
586. https://www.puntoseguro.com/seguros-de-vida/
587. https://www.coincrispy.com/2018/11/27/candidato-presidencial-nigeria-blockchain-mandato/
588. https://es.cointelegraph.com/news/dao-empresas-innovadoras-basadas-en-blockchain
589. https://www.pointnurse.com/blog/cyrus-maaghul-healthcare-blockchains-smart-contracts-and-daos/
590. https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/
591. https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/
592. https://www.coincrispy.com/2018/11/27/codigo-de-conducta-para criptomonedas/?utm_medium=pushnotes
593. https://medium.com/evernym/is-self-sovereign-identity-ssi-the-ultimate-gdpr-compliance-tool-9d8110752f89
594. https://alastria.io/assets/docs/responsabilidad.docx
595. https://uhx.io/wp-content/uploads/UHCWhitePaper-V2.3.pdf
596. http://prevenblog.com/blockchain-una-tecnologia-disruptiva-que-llega-para-cambiar-la-seguridad-y-salud-laboral/
597. https://www.quironprevencion.com/blogs/es/prevenidos/importancia-epi-prevencion-riesgos-laborales
598. https://blog.fichareneltrabajo.com/
599. https://beiota.com/
600. http://ec.europa.eu/trade/policy/in-focus/conflict-minerals-regulation/regulation-explained/index_es.htm
601. https://es.ihodl.com/analytics/2018-03-14/como-el-blockchain-ayudara-acabar-con-los-diamantes-de-sangre/
602. https://www.pwc.com/gx/en/sustainability/assets/blockchain-for-a-better-planet.pdf
603. FDA probará tecnología blockchain para el rastreo de suministro de medicinas. Vid https://www.coincrispy.com/2019/02/11/fda-probara-blockchain-medicinas/?utm_medium=pushnotes
604. https://guardtime.com/blog/blockcloud-re-inventing-cloud-with-blockchains
605. EDPS. (2016). *Annual Report*. Recuperado de https://edps.europa.eu/sites/edp/files/publication/17-04-27_annual_report_2016_en_1.pdf
606. https://datos.gob.es/sites/default/files/doc/file/orientaciones_y_garantias_anonimizacion_0.pdf
607. https://static1.squarespace.com/static/57c55d71725e25ba4eb91756/t/58e533fb1b631bedcc67acad/1491416088875/Salus+coop.pdf
608. www.bitcoin.org
609. http://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/Guia-encargado-del-tratamiento-RGPD-CAST.pdf
610. https://bitcoin.stackexchange.com/questions/59220/what-is-the-difference-between-a-miner-and-a-full-node

611. https://www.coincrispy.com/2019/04/02/regulador-china-companias-blockchain-aprobadas/?utm_medium=pushnotes
612. http://www.globaltimes.cn/content/1144347.shtml
613. https://eprint.iacr.org/2013/507.pdf
614. https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/
615. https://www.grantthornton.es/globalassets/___spain___/folletos/rgpd-y-blockchain-final.pdf
616. https://www.grantthornton.es/globalassets/___spain___/folletos/rgpd-y-blockchain-final.pdf
617. https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/
618. https://enigma.co/
619. Zyskind ; Oz Nathan ; Alex 'Sandy' Pentland . *ecentralizing Privacy: Using Blockchain to Protect Personal Data.* Recuperado de https://s3.amazonaws.com/enigmaco-website/uploads/pdf/ZNP15.pdf
620. Mainelli, M. Blockchain podría ayudarnos a recuperar el control sobre nuestros datos personales Recuperado de https://hbr.org/2017/10/smart-ledgers-can-help-us-reclaim-control-of-our-personal-data
621. https://thenextweb.com/hardfork/2018/12/14/blockchains-privacy-by-design-gdpr/
622. https://www.embleema.com/faq/
623. https://www.embleema.com/wp-content/uploads/2018/10/GDPR-Data-Processing-Addendum.pdf
624. https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf
625. https://ipfs.io/
626. Back, A. et al. (2014) *Enabling Blockchain Innovations with Pegged Sidechains*. Recuperado de https://blockstream.com/sidechains.pdf
627. https://martechtoday.com/venzee-launches-first-middleware-optimize-blockchain-bound-data-207051
628. Queen Mary University of London (6 de noviembre de 2018). *Are blockchains compatible with data privacy law?*. Recuperado de https://www.qmul.ac.uk/media/news/2018/hss/are-blockchains-compatible-with-data-privacy-law.html
629. Pérez Campillo, L. (2017). Novedades del nuevo GDPR en cloud computing. *ITUsers.* Recuperado de https://blogs.itdmgroup.es/lorena-p-campillo/2017/04/novedades-del-nuevo-gdpr-en-cloud-computing-mas-sombras-que-luces
630. RRI Tools (28 febrero 2019). Salus.coop, un marco para un enfoque dirigido por los ciudadanos a la gestión y gobernanza colaborativa de los datos de salud. Recuperado de https://www.rri-tools.eu/-/salus-coop-a-framework-for-a-citizen-led-approach-to-the-collaborative-managing-amp-governance-of-health-data
631. http://www.myhealthmydata.eu/tag/ehealth/
632. https://www.cio.com/article/3206607/what-is-grc-and-why-do-you-need-it.html
633. https://cuadernosdeseguridad.com/2018/04/alertan-del-incremento-de-ciberataques-a-equipos-medicos-en-2018/
634. https://www.technologyreview.es/s/5591/el-hospital-secuestrado-por-un-ciberataque-ha-pagado-el-rescate-de-15000-euros
635. https://www.eldiario.es/theguardian/fabricante-vibradores-indemnizar-clientes-espiarles_0_622238697.html
636. Centre for Information Policy Leadership , *CIPL (21 de diciembre de 2016). Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR. Recuperado de https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf*
637. Malin B. (2017) Quantitative Methods to Measure the Risk of Re-identification: Methodology Review. Recuperado de https://www.ema.europa.eu/en/documents/presentation/presentation-quantitative-methods-measure-risk-re-identification-b-malin_en.pdf
638. https://www.informationpolicycentre.com/
639. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/risk_webinar__24_may_2016_.pdf

640. http://www.thiber.org/wp-content/uploads/2016/06/sic120-ciberseguros.pdf https://obamawhitehouse.archives.gov/files/documents/cyber/ISA%20-%20Cyber-Insurance%20Metrics%20and%20Impact%20on%20Cyber-Security.pdf
641. Power Data. *El gobierno de datos eficaz. La guía para minimizar errores y alcanzar objetivos de gobernanza de datos.* Recuperado de https://cdn2.hubspot.net/hubfs/239039/docs/Ebook-Gobierno-Datos-Eficaz.pdf?t=1495399698278
642. Oñate, J. La clave para compartir información del sector público. *Revista Dintel* número 34. Recuperado de http://www.revistadintel.es/Revista1/DocsNum34/PersEmpresarial/Onate.pdf . En Puyol, J. (20 de noviembre de 2016).
643. Nanopdf (19 de marzo de 2018). *Código TIPO sectorial de Investigación Clinica y Farmacovigilancia.* Recuperado de https://nanopdf.com/download/codigo-tipo-sectorial-de-investigacion-clinica-y-farmacovigilancia_pdf
644. Stolker-Walker, C. (14 noviembre 2018). Why Google consuming DeepMind Health is scaring privacy experts. *Wired.* Recuperado de https://www.wired.co.uk/article/google-deepmind-nhs-health-data
645. https://revistapymes.es/eurocloud-crea-un-codigo-de-buenas-practicas-para-dar-mayor-seguridad-a-los-usuarios-de-la-nube/
646. https://cispe.cloud/code-of-conduct/.
647. http://www.dealerworld.es/cloud/primer-codigo-de-conducta-europeo-adoptado-por-proveedores-cloud
648. Pérez Campillo, L. (2017). Códigos de conducta y best practices en cloud computing. Recuperado de https://blogs.itdmgroup.es/lorena-p-campillo/2017/01/codigos-de-conducta-y-best-practices-en-cloud-computing-lo-que-esta-por-llegar
649. http://download.microsoft.com/download/F/9/9/F998F8EB-038A-4EEE-8B36-4B87362DBE96/Spanish_Spain.pdf
650. https://www.youtube.com/watch?v=1K5Ji_Kf1F8
651. https://resilience.enisa.europa.eu/cloud-computing-certification.
652. http://www.cesg.gov.uk/Publications/Documents/cesg-vmware_joint-statement14-09- 11.pdf
653. https://www.european-privacy-seal.eu/EPSen/Criteria.
654. https://www.juntadeandalucia.es/agenciadecalidadsanitaria/informe/2018/T3/centros/AppAPP.html
655. http://www.calidadappsalud.com/distintivo/catalogo
656. https://www.ixquick.com/esp/press/eu-privacy-seal.html?hmb=1
657. https://www.microsoft.com/es-xl/TrustCenter/Privacy/You-are-in-control-of-your-data
658. https://www.iso.org/obp/ui/#iso:std:iso-iec:19086:-1:ed-1:v1:en
659. https://en.wikipedia.org/wiki/ISO/IEC_27552
660. https://www.linkedin.com/feed/update/urn:li:ugcPost:6494233359500345344/
661. https://eurocloud.org/streams/staraudit/
662. https://ico.org.uk/media/1540/cloud_computing_guidance_for_organisations.pdf.
663. .https://www.academia.edu/11420153/El_Data_Protection_Officer_en_el_marco_de_la_responsabilidad_penal_de_las_personas_jur%C3%ADdicas_Consideraciones_a_la_luz_del_nuevo_Reglamento_Europeo_en_materia_de_protecci%C3%B3n_de_datos
664. https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Circular_1-2016.pdf?idFile=81b3c940-9b4c-4edf-afe0-c56ce911c7af.**)**
665. http://ecixgroup.com/el-grupo/compliance-como-una-nueva-forma-de-cultura-corporativa/
666. http://ecixgroup.com/el-grupo/hacia-una-nueva-institucion-el-compliance-por-diseno/
667. http://www.ciospain.es/cloud/el-25-de-los-directivos-no-sabe-quien-es-responsable-de-garantizar-la-privacidad-de-los-datos
668. https://www.ecixgroup.com/iso-19600-la-hoja-de-ruta-del-cumplimiento-normativo/
669. https://assets.kpmg/content/dam/kpmg/es/pdf/2018/07/estandares-internacionales-compliance.pdf pp 10
670. EFE (11 de septiembre 2008). Alemania multa con 1,5 millones de euros a Lidl por espiar a su empleados. *El País Economía.* Recuperado de https://elpais.com/economia/2008/09/11/actualidad/1221118375_850215.html

671. Bonatti, F. *Delitos contra la intimidad - Protección de los datos personales y familiares reservados. El "espionaje" personal y corporativo.* Recuperado de
672. https://www.bonattipenal.com/delitos-contra-la-intimidad-proteccion-de-los-datos-personales-y-familiares-reservados-el-espionaje-personal-y-corporativo/
673. https://www.elconfidencialdigital.com/media/elconfidencialdigital/files/2017/04/08/ECDFIL20170408_0001.pdf
674. NuevaTribina (11 de abril de 2017). Boeringher, nuevamente en la picota. Recuperado de https://www.nuevatribuna.es/articulo/sanidad/boehringer-nuevamente-picota/20170411175606138694.amp.html
675. https://es.wikipedia.org/wiki/Olodaterol
676. https://cuadernosdeseguridad.com/2018/04/alertan-del-incremento-de-ciberataques-a-equipos-medicos-en-2018/
677. https://interprofesionalgranada.files.wordpress.com/2017/09/comunicado-a-la-presidencia-y-consejeria-de-salud-de-la-junta-de-andalucia.pdf
678. Campos, C. (2018). *Compliance en el Sector Público ¿necesidad o virtud?*. Recuperado de http://concepcioncampos.org/compliance-en-el-sector-publico-necesidad-o-virtud/ (La autora utiliza el concepto del "compliance público").
679. http://www.diarioabierto.es/291570/jorge-salgueiro-la-autorregulacion-es-necesaria-hasta-que-los-mercados-maduren
680. https://www.agpd.es/portalwebAGPD/common/FOLLETO.pdf
681. https://es.wikipedia.org/wiki/Green_computing
682. Ponce de León, M. (7 de marzo de 2019). El supervisor europeo abre la puerta a la obligatoriedad de los ciberseguros. Recuperado de http://www.expansion.com/empresas/banca/2019/03/07/5c80277122601d7b6b8b45e8.html
683. https://www.tercerainformacion.es/articulo/internacional/2019/03/03/facebook-desarrollo-una-operacion-global-de-lobby-para-atacar-a-las-leyes-de-proteccion-de-datos
684. Vanin, N. [Nicola Vanin]. (20 de marzo, 2019). #Belgio, l'associazione che riunisce le industria belghe hashtag#FEB/ VBO ha presentato ricorso contro la legge che attua il Regolamento generale sulla protezione dei dati dell'UE hashtag#GDPR presso la corte costituzionale. [Tuit]. Recuperado de https://www.linkedin.com/feed/update/urn:li:activity:6514046252794155008/
685. Diario de Navarra. (22 de febrero de 2012). Salud debe pagar 125.000 euros por acceso ilegítimo historial una paciente. https://www.diariodenavarra.es/noticias/navarra/mas_navarra/salud_debe_pagar_125_000_euros_por_acceso_ilegitimo_historial_una_paciente_70815_2061.html
686. CORNOCK, Marc (2014) https://oro.open.ac.uk/49089/3/Legal%20principles%20of%20responsibility%20and%20accountability%20in%20healthcare.pdf
687. https://almacendederecho.org/sanciones-administrativas-y-responsabilidad-civil/
688. https://medium.com/@hackylawyER/money-talks-how-digital-money-speech-challenge-existing-legal-frameworks-dd845a7ceaf7
689. https://medium.com/@hackylawyER/do-we-really-want-to-sell-ourselves-the-risks-of-a-property-law-paradigm-for-data-ownership-b217e42edffa
690. http://hudoc.echr.coe.int/eng?i=001-162581
691. https://d-lab.tech/challenge-2/
692. https://www.statista.com/statistics/433871/daily-social-media-usage-worldwide/
693. https://confilegal.com/20190417-la-union-europea-aprueba-la-directiva-de-proteccion-a-los-denunciantes-de-corrupcion-o-whistleblowers/
694. https://www.eetimes.com/author.asp?section_id=36&doc_id=1330462
695. https://www.punto-informatico.it/rodot-il-corpo-umano-una-password/
696. http://www.privacy.it/archivio/rodo20040916.html
697. https://www.red.es/redes/es/sala-prensa/recursos-multimedia/pdfs/ponencia-de-stefano-rodot%C3%A0-para-el-conversatorio-sobre-derechos

698. http://www.camera.it/application/xmanager/projects/leg17/commissione_internet/dichiarazione_dei_diritti_internet_pubblicata.pdf
699. https://www.immedicohospitalario.es/noticia/15601/la-inteligencia-artificial-amenaza-la-privacidad-de-los-datos-de-salud
700. Comisión Europea (20 de noviembre 2018). Nube Europea de Ciencia Abierta (EOSC). Recuperado de https://ec.europa.eu/research/openscience/index.cfm?pg=open-science-cloud
701. European Data Portal (2018) Open Data Maturity in Europe. Recuperado de https://www.europeandataportal.eu/sites/default/files/edp_landscaping_insight_report_n4_2018.pdf
702. http://transparencia.gob.es/servicios-buscador/buscar.htm?categoria=estadistica&ente=E04921901&historico=false&lang=es
703. https://analisi.transparenciacatalunya.cat/browse?tags=salut
553. Verhulst, S., Noveck, B., Caplan, R., Brown, K., Paz, C. (mayo 2014). The open data Era in Health and Social Care. *GOBLAB NHS England.* Recuperado de www.thegovlab.org/static/files/publications/nhs-full-report.pdf
705. Kuo, L. (11 marzo 2019). *La base de datos de China enumera el estado de "raza" de 1,8 millones de mujeres.* The Guardian. Recuperado de https://www.theguardian.com/world/2019/mar/11/china-database-lists-breedready-status-of-18-million-women
706. Agència de Qualitat i Avaluació Sanitàries de Catalunya – Generalitat de Catalunya. Dep. de Salut. Reutilización de la información para mejorar la investigación y la evaluación de los servicios sanitarios. Recuperado de www.fundacio.udl.cat/biobancos/doc/sesiones/Sesion4-RamonMaspons.pdf
707. https://datos.gob.es/es/documentacion/orientaciones-y-garantias-en-los-procedimientos-de-anonimizacion-de-datos-personales
708. RedacciónMédica (12 de febrero de 2018). "La LOPD obvia el papel del Comité de Ética en la investigación oncológica". Recuperado de https://www.redaccionmedica.com/secciones/oncologia-medica/-la-lopd-obvia-el-papel-del-comite-de-etica-en-la-investigacion-oncologica--6934
709. https://ssd.eff.org/es/module/por-qu%C3%A9-los-metadatos-son-importantes
710. Elvery, S. (3 de diciembre de 2018). Mis dispositivos envían y reciben datos cada dos segundos, a veces incluso cuando duermo. *ABC NET AU.* Recuperado de https://www.abc.net.au/news/2018-11-16/datalife-i-spied-on-my-phone-and-here-is-what-i-found/10496450?pfmredir=sm
711. Romero, P. (28 enero de 2019). ¿Quién nos protege de nuestros metadatos?. *Público*. Recuperado de https://www.publico.es/sociedad/proteccion-datos-metadatos.html
712. https://github.com/ricochet-im/ricochet
713. Comisión Europea (21 enero de 2019) Primeros ciudadanos de la UE que utilizan recetas electrónicas de la UE. Recuperado de http://europa.eu/rapid/press-release_IP-18-6808_en.htm
714. Comisión Europea. eSalud: salud y atención digital. Recuperado de https://ec.europa.eu/health/ehealth/policy/network_en
715. Consejo de Europa (28 de marzo de 2019). Protection of health-related data: new guidelines. Recuperado de https://www.coe.int/en/web/human-rights-rule-of-law/home/-/asset_publisher/1qETLXmIMIRe/content/protection-of-health-related-data-new-guidelines?_101_INSTANCE_1qETLXmIMIRe_viewMode=view
716. https://www.washingtonpost.com/technology/2019/02/27/us-government-fined-app-now-known-tiktok-million-illegally-collecting-childrens-data/?utm_term=.502fca43e2f9
717. https://www.ftc.gov/system/files/documents/cases/musical.ly_complaint_ecf_2-27-19.pdf
718. Castelló, C. (11 de diciembre de 2013). El DNI de jóvenes cambia para evitar que mientan con su edad en internet. *CincoDías.* Recuperado de https://cincodias.elpais.com/cincodias/2013/12/10/empresas/1386690018_072015.html
719. Comisión Europea (junio de 2011). Eurobarómetro Especial 359. Attitudes on Data Protection and Electronic Identity in the European Union. Recuperado de http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf
720. Grupo de expertos de múltiples partes interesadas para apoyar la aplicación del Reglamento (UE) 2016/679 (E03537). Recuperado de http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537

721. Comisión Europea. Secciones Horizonte 2020. Recuperado de https://ec.europa.eu/programmes/horizon2020/h2020-sections
722. Comisión Europea (8 de noviembre de 2018). Answer by Ms. Jourovà on behalf of the European Commission. Recuperado de http://www.europarl.europa.eu/doceo/document/E-8-2018-004999-ASW_EN.pdf
723. Noticias Jurídicas. (18 de marzo de 2019). La AEPD es competente para sancionar a una entidad con sede en Luxemburgo y con apartado de correos y cuenta bancaria en España. Recuperado de *NoticiasJurídicas.* Recuperado de http://noticias.juridicas.com/actualidad/jurisprudencia/13789-la-aepd-es-competente-para-sancionar-a-una-entidad-con-sede-en-luxemburgo-y-con-apartado-de-correos-y-cuenta-bancaria-en-espana/
724. https://www.eldiario.es/sociedad/delito_de_revelacion_de_secretos_0_854965182.html
725. Adsuara, B. (31 de enero de 2019). ¿Y por qué no una Mediación en Protección de Datos? La Información. Recuperado de https://www.lainformacion.com/opinion/borja-adsuara/y-por-que-no-una-mediacion-en-proteccion-de-datos/6491255/
726. García Herrero, J. (16 de julio de 2018). Sí se puede! Datos de categoría especial tratados sobre interés legítimo.Recuperado de https://jorgegarciaherrero.com/datos-de-categoria-especial-tratados-sobre-interes-legitimo/
727. https://www.sanitas.es/contratacionservicios/textoLegal?mostrarFancyPoliticaPrivacidad#terceraspartes_hospitales
728. Van Quathem K. (13 de febrero de 2019). *El Consejo Europeo de Protección de Datos publica una guía sobre la intersección del GDPR y el Reglamento de ensayos clínicos*. Recuperado de
729. https://www.insideprivacy.com/eu-data-protection/european-data-protection-board-releases-guidance-on-intersection-of-the-gdpr-and-the-clinical-trials-regulation/
730. Cabo Salvador, J. *Los sistemas sanitarios y sus objetivos.* Udima. Recuperado de https://www.gestion-sanitaria.com/1-sistemas-sanitarios-objetivos.html.
731. https://www.sanitas.es/contratacionservicios/textoLegal?mostrarFancyPoliticaPrivacidad
732. https://www.aepd.es/areas/internet/derecho-al-olvido.html
733. El Abogado General Szpunar propone al Tribunal de Justicia que declare que los gestores de motores de búsqueda deben aceptar sistemáticamente las solicitudes de desreferenciación de datos sensibles. Recuperado de https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-01/cp190001es.pdf
734. https://www.aepd.es/reglamento/cumplimiento/transferencias-internacionales.html
735. https://www.elmundo.es/economia/empresas/2019/01/22/5c47118bfc6c83384a8b45e9.html
736. AI Now (diciembre 2018). Report 2018. Recuperado de https://ainowinstitute.org/AI_Now_2018_Report.pdf
737. RedaccionMédica (22 de febrero de 2018). Protección de datos: "Las enmiendas sanitarias a la LOPD no son necesarias". Recuperado de https://www.redaccionmedica.com/secciones/derecho/proteccion-de-datos-las-enmiendas-sanitarias-a-la-lopd-no-son-necesarias--7480
738. García, J. (19 de noviembre de 2017). La Inteligencia Artificial ha evitado que me suicidara. *El País. La Retina.* Recuperado de https://retina.elpais.com/retina/2017/11/17/innovacion/1510908438_438297.html
739. https://www.ecured.cu/Investigaci%C3%B3n_cient%C3%ADfica
740. https://www.newscientist.com/article/2086454-revealed-google-ai-has-accessto-huge-haul-of-nhs-patient-data/.
741. D'Acquisito, Giuseppe et al. (2015). Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics. Pag. 46. *ENISA*, Recuperado de https://arxiv.org/ftp/arxiv/papers/1512/1512.06000.pdf
742. http://www.bdo.co.uk/__data/assets/pdf_file/0011/1350101/BDO_HMRC_DIGITAL_AGE. pdf
743. http://www.europapress.es/portaltic/sector/noticia-sap-primera-tecnologica-europea-crear-grupo-asesor-etica-inteligencia-artificial-20180918182850.html
744. http://www.tellmegen.com/
745. https://www.eprivacidad.es/multa-a-un-hospital-por-compartir-datos-procedentes-de-aseguradoras-privadas-con-el-servicio-de-salud-gallego/
746. https://www.laverdad.es/murcia/denuncian-cita-previa-20190214003636-ntvo.html

747. CSA (2013). Expanded Top Ten Big Data Security and Privacy Challenges. Recuperado de https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Expanded_Top_Ten_Big_Data_Security_and_Privacy_Challenges.pdf
748. Álvarez Hazas, G.Anonimización de datos personales de la investigación. Perspectiva jurídica y práctica. Mallorca, 2018. Recuperado de https://gahazas.files.wordpress.com/2018/11/anonimizacic3b3n-de-datos-personales-para-investigacic3b3n_v3.pdf
749. https://www.england.nhs.uk/2013/10/care-data/
750. Welcome. Ac.Uk. Ensuring the effective use of patient data. Recuperado de https://wellcome.ac.uk/sites/default/files/ensuring-the-effective-use-of-patient-data-briefing-aug15.pdf.
751. https://translate.google.es/translate?hl=es&sl=fr&u=http://www.20minutes.fr/sante/1563619-20150316-droit-oubli-survivants-cancer-projet-loi-sante&prev=search
752. https://www.eldiario.es/sociedad/test_geneticos-ADN-privacidad-ciencia_0_869313773.html
753. Girard-Opicci, C. (10 de febrero de 2015). Los ex pacientes de cáncer o las personas con enfermedades crónicas pueden beneficiarse de un seguro de "derecho a olvidar". *Net-Iris*. Para más info aquí
754. https://es.wikipedia.org/wiki/Tecno%C3%A9tica
755. http://w2.vatican.va/content/leo-xiii/es/encyclicals/documents/hf_l-xiii_enc_20061888_libertas.html
756. https://es.wikipedia.org/wiki/Homo_Deus:_Breve_historia_del_ma%C3%B1ana
757. Peña Corrales, P. (19 de octubre de 2016). Dataísmo: ¿El albor de una religión digital?. *La Grieta*. Recuperado de http://lagrietaonline.com/dataismo-el-albor-de-una-religion-digital/
758. Geli, C. (7 de febrero de 2018). "Ahora uno se explota a sí mismo y cree que está realizándose". *El País*. Recuperado de https://elpais.com/cultura/2018/02/07/actualidad/1517989873_086219.html
759. HARARI, Yuval Noah (2016). Yuval Noah Harari on big data, Google and the end of free will. *Financial Times*. Recuperado de https://www.ft.com/content/50bb4830-6a4c-11e6-ae5b-a7cc5dd5a28c
760. https://www.washingtonpost.com/opinions/you-can-run-from-big-data-but-can-you-hide/2015/03/20/082ea46c-c805-11e4-a199-6cb5e63819d2_story.html?noredirect=on&utm_term=.cc5c1476d724
761. https://docs.google.com/presentation/d/1yq9JLBufrzBIyLW2OvZRDt50TCU5tNoNoHGtyNfqVgs/edit#slide=id.g3fddd1e893_0_143
762. https://docs.google.com/presentation/d/1yq9JLBufrzBIyLW2OvZRDt50TCU5tNoNoHGtyNfqVgs/edit#slide=id.g3fffc0c23d_0_0
763. *TED. Dave deBronkart. Meet a e-Patient Dave.* Recuperado de https://www.ted.com/talks/dave_debronkart_meet_e_patient_dave
764. https://en.wikipedia.org/wiki/Dave_deBronkart
765. http://e-patients.net/archives/2009/04/imagine-if-someone-had-been-managing-your-data-and-then-you-looked.html
766. .https://journals.lww.com/lww-medicalcare/Citation/2019/02000/Inpatients_Sign_On__An_Opportunity_to_Engage.2.aspx
767. https://saludconcosas.blogspot.com/2019/01/informacion-en-tiempo-real-para.html;
768. Giessler, J. (14 de septiembre de 2018). Bedside app eased stress of hospital patientes. Recuperado de The Ohio State University. Wexner Medical Center. Recuperado de https://wexnermedical.osu.edu/blog/mychart-bedside
769. AHRQ Health Care Innovations Exchange (2008). "Las comunidades en línea fomentan el intercambio de datos, la comunicación y el aprendizaje entre pacientes con enfermedades neurológicas y otras enfermedades crónicas" . *AHRQ* Recuperado de https://innovations.ahrq.gov/profiles/online-communities-foster-data-sharing-communication-and-learning-among-patients-neurologic
770. https://www.eleconomista.es/sanidad/noticias/8144868/02/17/La-farmaceutica-Acorda-se-dispara-en-bolsa-por-su-nuevo-medicamento-contra-el-Parkinson.html

771. https://www.patientslikeme.com/clinical_trials/NCT01767129-levodopa-dyskinesia-parkinsons-disease-AVP-923-dextromethorphan-quinidine
772. http://www.appliedclinicaltrialsonline.com/bbk-worldwide-and-patientslikeme-launch-online-diabetes-health-movement
773. https://blogs.plos.org/speakingofmedicine/2012/06/14/open-access-is-not-for-scientists-its-for-patients/
774. https://www.patientslikeme.com/about/partners
775. https://www.quora.com/How-much-are-pharma-companies-willing-to-pay-for-patientslikeme-data
776. Ortiz, P. (2018). La protección de datos, un asunto profundamente humano. Recuperado de http://theconversation.com/la-proteccion-de-datos-un-asunto-profundamente-humano-108137
777. Knight W. (9 de octubre de 2017). *MIT Technology Review.* Recuperado de https://www.technologyreview.es/s/9610/google-advierte-el-verdadero-peligro-de-la-ia-no-son-los-robots-asesinos-sino-los-algoritmos?_ga=2.180570592.690192898.1543855212-419410505.1543855212
778. https://www.gartner.com/newsroom/id/3144217
779. Mendoza Zabala, G. (2017). El papel de la filosofía en la era tecnológica. Recuperado de https://www.madrimasd.org/notiweb/analisis/papel-filosofia-en-era-tecnologica
780. https://cis-india.org/papers/ebola-a-big-data-disaster
781. http://eterni.me/
782. https://www.forbes.com/sites/enriquedans/2018/09/21/insurance-wearables-and-the-future-of-healthcare/#27449a671782
783. https://datanews.knack.be/ict/nieuws/een-nieuw-jaar-een-nieuwe-ai/article-opinion-1412987.html?cookie_check=1546692144
784. https://retina.elpais.com/retina/2019/01/04/tendencias/1546604928_551805.amp.html M.Luengo
785. https://www.eldiario.es/tecnologia/CE-avanza-directrices-inteligencia-artificial_0_783572209.html#click=https://t.co/wrGOHMuiFM
786. https://www.bbc.com/mundo/noticias/2015/07/150702_tecnologia_google_perdon_confundir_afroamericanos_gorilas_lv
787. https://elpais.com/elpais/2017/09/19/ciencia/1505818015_847097.html
788. https://www.xataka.com/privacidad/durante-2018-17-5-millones-ciudadanos-chinos-no-pudieron-comprar-billete-avion-tener-credito-social
789. https://amp.infosalus.com/asistencia/noticia-inteligencia-artificial-amenaza-creciente-privacidad-datos-salud-20190104121513.html
790. https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2719130
791. https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2719121
792. https://www.instagram.com/p/BqfJIQDhLmr/?utm_source=ig_share_sheet&igshid=rbin43g4igsn
793. https://psyarxiv.com/hv28a/
794. https://elpais.com/tecnologia/2018/01/14/actualidad/1515955554_803955.html
795. https://www.wired.com/story/facebooks-chatbots-will-not-take-over-the-world/
796. CNIL. (26 de diciembre de 2017). How can humans keep the upper hand? Report on the ethical matters raised by algorithms and artificial intelligence**.** Recuperado de https://www.cnil.fr/en/how-can-humans-keep-upper-hand-report-ethical-matters-raised-algorithms-and-artificial-intelligence
797. Tranberg, P. (19 octubre de 2018). Debating ethics: We need a "manual override" button. *DataEthics.* Recuperado de https://dataethics.eu/en/debating-ethics-we-need-manual-override/
798. Comisión Europea. The European AI Alliance. Recuperado de https://ec.europa.eu/digital-single-market/en/european-ai-alliance
799. https://www.aclu.org/issues/privacy-technology/surveillance-technologies/algorithms-are-making-government-decisions
800. https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf
801. https://www.aclu.org/issues/privacy-technology/surveillance-technologies/ai-engineers-must-open-their-designs-democratic?redirect=issues/privacy-technology/consumer-privacy/ai-engineers-must-open-their-designs-democratic-control

802. https://www.aclu.org/issues/privacy-technology/surveillance-technologies/algorithms-are-making-government-decisions
803. https://9to5mac.com/2018/06/04/apple-opens-health-records-api-for-developers/
804. https://www.revistagq.com/noticias/tecnologia/articulos/apple-watch-series-4-critica-caracteristicas-opiniones/30946
805. https://www.tribuna.com.mx/cienciaytecnologia/Nueva-herramienta-en-el-Apple-Watch-salva-la-vida-de-una-persona-20181209-0083.html
806. https://elchapuzasinformatico.com/2018/05/un-apple-watch-salva-la-vida-a-un-hombre-tras-detectar-una-ulcera-perforada/
807. https://dataethics.eu/en/fitnesstrackersleak/
808. https://www.ituser.es/movilidad/2015/05/el-31-de-las-aseguradoras-utiliza-wearables-para-comunicarse-con-clientes-empleados-y-socios
809. https://www.reuters.com/article/us-manulife-financi-john-hancock-lifeins/strap-on-the-fitbit-john-hancock-to-sell-only-interactive-life-insurance-idUSKCN1LZ1WL
810. http://www.forbes.com/sites/brucejapsen/2015/02/08/anthem-cyber-attack-clouds-insurers-obamacare-bounty/
811. http://www.techtimes.com/articles/69953/20150718/ucla-health-data-breach-affects-4-5-million-patients-what-you-should-know.html
812. https://www.ncbi.nlm.nih.gov/pubmed/25713012
813. https://www.researchgate.net/publication/275413868_Security_and_Privacy_Issues_in_Implantable_Medical_Devices_A_Comprehensive_Survey
814. http://www.intotheminds.com/blog/en/30-days-to-read-privacy-policies-consent-fatigue-will-make-gdpr-ineffective/
815. https://retina.elpais.com/retina/2017/07/04/tendencias/1499160204_361460.html
816. https://www.linkedin.com/feed/update/urn:li:activity:6521620270313275392/.
817. The Futurist. (20 enero 2019). Japanese researchers are teaching mobile phones how to read minds by scanning brain waves!". Recuperado de https://twitter.com/thefuturist007/status/1087067132746219523?s=12
818. https://www.abc.es/ciencia/abci-ignacio-cirac-estamos-puertas-segunda-revolucion-cuantica-201705052018_noticia.html
819. http://content.time.com/time/specials/packages/0,28757,2019341,00.html
820. https://www.technologyreview.es/s/10632/riesgos-de-la-salud-20-si-quiere-ver-al-medico-debera-ceder-sus-datos
821. https://medium.com/s/story/your-privacy-is-over-ed72d06418f1
822. https://static1.squarespace.com/static/57c55d71725e25ba4eb91756/t/58e533fb1b631bedcc67acad/1491416088875/Salus+coop.pdf
823. XXIII Jornadas Nacionales de Informática Sanitaria en Andalucía 'Innovación y Salud', un evento organizado por la Sociedad Española de Informática de la Salud (SEIS). Ver artículo http://www.elmedicointeractivo.com/articulo/reportajes/big-data-sanitario-herramienta-aun-desconocida/20161025143034106859.html
824. Valdivieso, B. y Peiró, S. Presentación del informe *"Big data y Salud"* Planner Meida y Prodigioso Volcán, Roche Farma y Siemens. Recuperado de http://haycanal.com/noticias/8617/Big-Data--Los-datos-en-salud-pueden-salvar-vidas
825. https://drive.google.com/drive/folders/1FJ1hnK8sO-7WD7VTVsZ81t4jHn8uYD6e
826. https://retina.elpais.com/retina/2019/01/04/tendencias/1546604928_551805.amp.html
827. https://medium.com/@hackylawyER/money-talks-how-digital-money-speech-challenge-existing-legal-frameworks-dd845a7ceaf7
828. https://medium.com/@hackylawyER/do-we-really-want-to-sell-ourselves-the-risks-of-a-property-law-paradigm-for-data-ownership-b217e42edffa
829. https://www.youtube.com/watch?v=d36eDT4lPWc
830. https://www.scu.edu/ethics/internet-ethics-blog/on-data-ethics-an-interview-with-shannon-vallor/
831. https://www.pointnurse.com/blog/do-you-have-a-healthcare-blockchain-strategy/

832. https://ec.europa.eu/digital-single-market/en/news/final-results-european-data-market-study-measuring-size-and-trends-eu-data-economy
833. https://s21.q4cdn.com/399680738/files/doc_financials/2017/Q4/Q4-2017-Earnings-Presentation.pdf
834. https://www.eldiario.es/tecnologia/cotizan-mercado-Facebook-precio-fluctua_0_757675161.html#click=https://t.co/uwAnl74Len
835. http://testdeprivacidad.org/?page=iframe
836. https://www.technologyreview.es/s/7332/los-datos-geneticos-de-23andme-valen-2500-veces-mas-por-usuario-que-los-de-facebook
837. http://www.forbes.com/sites/matthewherper/2015/01/06/surprise-with-60-million-genentech-deal-23andme-has-a-business-plan/
838. https://www.eldiario.es/hojaderouter/seguridad/hospitales-sanidad-seguridad_informatica-ciberataques-datos-privacidad_0_427657312.html
839. https://www.cbsnews.com/news/do-hackers-have-your-health-records/
840. https://www.mcafee.com/es/resources/reports/rp-hidden-data-economy.pdf
841. https://threatpost.com/deceased-patient-data-being-sold-on-dark-web/133871/
842. https://www.aarp.org/money/scams-fraud/info-03-2013/protecting-the-dead-from-identity-theft.html
843. https://www.theregister.co.uk/2018/06/13/royal_free_deepmind_deal_audit/
https://www.openhumans.org/
845. DERES."Manual para elaborar CÓDIGOS DE ÉTICA EMPRESARIAL", Uruguay. Recuperado de http://deres.org.uy/wp-content/uploads/Manual-de-Etica-DERES.pdf
846. https://elpais.com/tecnologia/2016/06/22/actualidad/1466608415_759681.html
847. Fernández, R. (2011). Códigos éticos o de conducta. Su concepto. Su necesidad. *Diario Responsable*. Recuperado desde http://diarioresponsable.com/opinion/14404-codigos-eticos-o-de-conducta-su-conceptosu-necesidad
848. http://panzi.github.io/SocialSharePrivacy/
849. https://dataethics.eu/en/tools/
850. https://probonoaustralia.com.au/news/2018/11/ethical-trust-mark-promotes-fair-data-use-australian-businesses/
851. http://fairdata.com.au/the-10-fair-data-principles-consumer/
852. http://www.tristanharris.com/the-need-for-a-new-design-ethics/
853. http://humanetech.com/problem#the-way-forward
854. https://planetachatbot.com/el-papel-de-la-%C3%A9tica-del-dise%C3%B1o-y-las-consecuencias-imprevistas-del-2017-33190df0637
855. https://elpais.com/tecnologia/2013/04/10/actualidad/1365620520_279623.html
856. https://www.elespanol.com/economia/empresas/20190128/facebook-lanza-centro-recursos-privacidad-empresas/371963142_0.html
857. https://www.technologyreview.es/s/10266/no-podemos-permitirnos-usar-inadecuadamente-los-datos-del-paciente
858. https://dataethics.eu/en/data-ethics-is-a-game-of-interests/
859. https://confilegal.com/20181223-la-etica-y-la-responsabilidad-derivada-del-uso-de-los-algoritmos/
860. https://dataethics.eu/en/data-ethics-is-a-game-of-interests/
861. https://confilegal.com/20181223-la-etica-y-la-responsabilidad-derivada-del-uso-de-los-algoritmos/
862. MICROSOFT (2014a): "Microsoft, en la lista de las Empresas Más Éticas del Mundo por cuarto año consecutivo". Recuperado de https://news.microsoft.com/esxl/microsoft-en-la-lista-de-las-empresas-mas-eticas-del-mundo-por-cuarto-anoconsecutivo/
863. https://www.ticbeat.com/cyborgcultura/swipe-buster-la-pagina-que-comprueba-si-tu-pareja-esta-en-tinder/
864. http://cdn2.hubspot.net/hubfs/319387/LRN_GCL_Brochure.pdf
865. https://es.weforum.org/agenda/2017/05/por-que-las-organizaciones-mas-exitosas-se-enfocan-en-valores/
866. https://www.ourworld.co/humanitys-finest-work-of-art/
867. https://static1.squarespace.com/static/57c55d71725e25ba4eb91756/t/58e533fb1b631bedcc67acad/1491416088875/Salus+coop.pdf

868. https://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps/
869. https://en.wikipedia.org/wiki/Barnaby_Jack
870. https://www.eldiario.es/hojaderouter/seguridad/Black_Hat-Def_Con-hackers-hacking-las_vegas_0_276122639.html
871. Stilgherrian (21 de octubre de 2011). "Hackeo de dispositivos médicos letales llevado al siguiente nivel" . CSO Online (Australia) . Recuperado de . https://www.cso.com.au/article/404909/lethal_medical_device_hack_taken_next_level/
872. https://www.blackhat.com/us-18/briefings/schedule/#understanding-and-exploiting-implanted-medical-devices-11733
873. https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/80-to-0-in-under-5-seconds-falsifying-a-medical-patients-vitals/
874. https://arxiv.org/abs/1901.03597
875. https://www.youtube.com/watch?v=_mkRAArj-x0
876. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/01/29/the-cybersecurity-202-medical-devices-are-woefully-insecure-these-hospitals-and-manufacturers-want-to-fix-that/5c4f4a661b326b29c3778cef/?utm_term=.f7488baac1fb.
877. https://healthsectorcouncil.org/the-joint-security-plan/
878. https://singularityhub.com/2019/02/26/quantum-computing-now-and-in-the-not-too-distant-future/
879. https://www.eae.es/actualidad/experto-en-blockchain-y-en-etica-de-datos-y-privacidad-las-posiciones-del-futuro-segun-el-informe-epyce
880. https://s3.ap-south-1.amazonaws.com/nhct.io/NHCT_Whitepaper.pdf
881. http://whitepaper.embleema.com/
882. https://www.grantthornton.es/globalassets/ spain /folletos/rgpd-y-blockchain-final.pdf
883. https://www.healthcareitnews.com/news/how-blockchain-can-help-healthcares-patient-matching-problem
884. https://blogs.itdmgroup.es/lorena-p-campillo/2017/01/cloud-computing-homologacion-de-proveedores-cloud-y-data-protection
885. https://confilegal.com/20170118-puyo-javier-cumplimiento-normativo/
886. https://www.beiota.com/
887. https://blogs.iadb.org/salud/es/tecnologias-cuanticas/?fbclid=IwAR3qOOmjmw7OSqTrpipx353wB97jgWdbbYjN2uB3eWv_m3_yVEmac59X56A